(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 855**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
A61B 5/00 (2006.01)
H04L 29/08 (2006.01)
G06F 19/00 (2011.01)
G06F 21/62 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.06.2009 PCT/IB2009/052471**

(87) Fecha y número de publicación internacional: **23.12.2009 WO09153710**

(96) Fecha de presentación y número de la solicitud europea: **10.06.2009 E 09766247 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.08.2016 EP 2291977**

(54) Título: **Administrador de seguridad personal para la monitorización omnipresente de los pacientes**

(30) Prioridad:

18.06.2008 EP 08104451

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.02.2017

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

GARCIA MORCHON, OSCAR;
HUEBNER, AXEL, G. y
BALDUS, HERIBERT

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Administrador de seguridad personal para la monitorización omnipresente de los pacientes

La presente invención se refiere a sistemas de seguridad electrónicos. Más particularmente, la invención se refiere a un aparato y un procedimiento correspondiente para el acceso y la monitorización seguros de la asistencia sanitaria.

Antecedentes de la invención

Las redes de sensores inalámbricos se despliegan cada vez más para la monitorización de la salud, lo cual lleva a los sistemas de monitorización de pacientes omnipresentes. En estos sistemas, cada paciente lleva una red de sensores corporales (BSN), que permite la monitorización de sus signos vitales en el hogar, los hospitales, o prácticamente en cualquier lugar. En este contexto, un paciente puede monitorizarse en muy diferentes escenarios y con diferentes conjuntos de dispositivos o nodos de sensores médicos.

Las tecnologías de sensores y comunicación inalámbrica están evolucionando rápidamente y conquistan nuevas áreas de aplicación, tales como la asistencia sanitaria. Los sensores médicos inalámbricos (WMS) son cada vez más pequeños y potentes, lo que permite un uso omnipresente para una amplia gama de aplicaciones médicas, tales como la gestión de enfermedades crónicas. En un entorno sanitario típico, un conjunto de WMS que proporcionan mediciones de una variedad de parámetros, por ejemplo, ECG, SpO_2 y la presión arterial, forma la red de sensores corporales del usuario (BSN), lo cual permite la monitorización de la salud, la medición de los signos vitales de un usuario y el envío de su información de salud electrónica (EHI) a una puerta, como un teléfono móvil. La puerta de entrada permite al usuario acceder directamente y procesar su EHI, y por otra parte, lo transmite, por ejemplo, a un proveedor de servicios de asistencia sanitaria, donde se almacena y se puede acceder a la misma o ser modificada por las partes autorizadas, tales como personal médico, familia, o entrenadores deportivos.

El uso omnipresente de BSN permite la monitorización de la salud en los entornos habituales de los usuarios, por ejemplo, en casa o durante el entrenamiento, y por lo tanto, mejora la calidad de la asistencia sanitaria y el bienestar de los usuarios, y al mismo tiempo permite una reducción de costes en el sector sanitario. La monitorización de la salud sanitaria en estas diversas situaciones y lugares se lleva a cabo por parte de diferentes organizaciones, tales como consultorios, gimnasios, hospitales o residencias de ancianos por medio de redes de sensores médicos (MSN). Una MSN comprende un gran número de WMS utilizados para monitorear los signos vitales de unos cuantos o muchos usuarios con sensores y algoritmos específicos de la enfermedad. Por lo tanto, las MSN tienen diferentes requisitos de funcionamiento con respecto a su tamaño, capacidades, o campo de aplicación. En una MSN, un subconjunto arbitrario de WMS puede estar asociado a un paciente para formar su BSN y supervisar su estado de salud en tiempo real. La EHI medida del usuario puede ser procesada por los WMS de la BSN o mediante un PDA clínico, o puede ser enviada a través de una puerta a una base de datos de MSN local o a los servicios de asistencia sanitaria finales, por ejemplo, el proveedor de servicios de asistencia sanitaria, el servicio de gestión de enfermedades, el servicio de registro de salud personal o el servicio de monitorización de implantes, para su posterior procesamiento.

Las MSN omnipresentes están desconectadas unas de otras, ya que pueden pertenecer a diferentes organizaciones. En consecuencia, los WMS que son diferentes de las MSN tal vez no sean interoperables a niveles de hardware y software debido a incompatibilidades técnicas, o a nivel de la organización debido a las diferentes políticas de seguridad. Sin embargo, la visión de la asistencia sanitaria omnipresente exige que todos los escenarios de aplicación MSN trabajen conjuntamente y estén conectados a servicios finales con el fin de permitir que los usuarios se muevan a través de MSN y para asegurar que su estado de salud puede ser monitoreado por personal autorizado de diferentes organizaciones, incluyendo hospitales o compañías de seguros.

El intercambio de datos médicos de los usuarios intra- e inter-MSN conlleva preocupaciones de privacidad y la seguridad que exigen servicios básicos de seguridad, por ejemplo, confidencialidad y autentificación. Estos servicios de seguridad deben garantizar la seguridad y privacidad de los pacientes, como es requerido por las alianzas de asistencia sanitaria como HITRUST, y deben cumplir con las directivas legales, como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) en los Estados Unidos y la directiva europea 95/46 sobre protección de datos. En particular, una EHI de usuario debe estar protegida de forma integral, es decir, de los WMS de su BSN a las bases de datos de MSN y servicios de asistencia sanitaria finales con el fin de evitar que personas no autorizadas tengan acceso a sus datos médicos. Sin embargo, proporcionar privacidad en un ambiente así es un reto debido a las características de MSN que incluyen: (I) movilidad inter e intra-MSN de los usuarios; (Ii) la naturaleza de recursos limitados de los WMS; (Iii) el hecho de que cualquier subconjunto de WMS de un conjunto de WMS de una MSN puede formar la BSN utiliza para controlar el estado de salud de un usuario; (Iv) y el requisito de identificación de BSN y usuario inequívoca en todo el sistema de MSN omnipresentes.

Los problemas de seguridad y privacidad se han abordado tanto para los servicios finales centralizados como para los escenarios de aplicación MSN aislados. Por ejemplo, se introdujo una infraestructura de seguridad XML para proporcionar control de acceso a EHI en la infraestructura de servicios finales. Se analizaron los problemas de

seguridad para redes de sensores inalámbricos en aplicaciones de asistencia sanitaria aisladas. Se han presentado los requisitos de seguridad y la infraestructura de los sistemas de información clínicos independientes. Sin embargo, el estado de la técnica carece de la definición de un sistema de seguridad integral, donde la BSN de un paciente se puede identificar de forma inequívoca en todo el sistema de las MSN omnipresentes, donde WMS se puede asociar a una red de área de paciente (PAN) de un paciente BSN de una manera segura y eficiente, y donde la seguridad integral puede proporcionarse mediante un enfoque de distribución de claves eficiente.

Es un reto cumplir con los estrictos requisitos de seguridad para aplicaciones médicas que son requeridos legalmente por las directivas como HIPAA. La seguridad y la privacidad de los datos médicos de un usuario deben garantizarse de forma integral, es decir, desde los nodos de sensores individuales hasta los servicios de asistencia sanitaria finales. Esto es particularmente difícil debido a las características de las redes de sensores médicos (MSN) omnipresentes, tales como: (I) soportar la movilidad intra- e inter-MSN de los pacientes (Ii) tener en cuenta la naturaleza de recursos limitados de sensores médicos; (Iii) formar una red de sensores corporales de un usuario a partir de cualquier subconjunto del conjunto de una red de sensores médicos de sensores médicos inalámbricos; y (iv) proporcionar una identificación de la red de sensores corporales y de usuarios inequívoca.

Un sistema de asistencia sanitaria omnipresente es aplicable a una amplia gama de escenarios de asistencia sanitaria y combina diversas tecnologías. A nivel organizativo, el sistema de asistencia sanitaria omnipresente puede dividirse en MSN controladas por diferentes instituciones, por ejemplo, hospitales, gimnasios, consultorios, o basadas en el hogar. En general, las MSN son redes distribuidas, a gran escala, ad hoc que funcionan de forma independiente. Las MSN pueden comprender un gran número de WMS asociados con diferentes pacientes y BSN. En general, solo los WMS asociados con el mismo paciente se comunican entre sí, de modo que las BSN están desconectadas. La movilidad tanto de nodos como de pacientes hace que la topología de MSN sea altamente dinámica. En la técnica anterior, a nivel de implementación, los WMS utilizados en diferentes MSN no son interoperables, y desde un punto de vista técnico y de seguridad, ya que tal vez no estén basados en tecnologías compatibles y pueden pertenecer a diferentes dominios de seguridad.

Con el fin de hacer que los WMS sean portátiles y para evitar que sean una carga para la vida diaria de un usuario, los WMS tienen que ser pequeños y ligeros. Como resultado de estas limitaciones de tamaño y peso, los WMS también están limitados en cuanto a vida útil de la batería, la memoria disponible y la potencia de cálculo. En este contexto, IEEE 802.15.4 y ZigBee son dos estándares clave debido a su bajo consumo de energía, la memoria y los requisitos computacionales, encajando con aplicaciones de red de área personal inalámbricas (PAN) o BSN de baja velocidad.

Debido a la gama de radio restringida de los WMSs que forman una BSN, los WMS tienen que contar con un dispositivo de puerta de enlace para garantizar la conectividad permanente a servicios de asistencia sanitaria finales remotos que gestionan, almacenan y dan acceso a los datos médicos del paciente. La comunicación entre puertas y servicios de asistencia sanitaria se puede lograr con medios inalámbricos para BSN móviles o con medios de cable para aplicaciones en un entorno restringido, cerrado, por ejemplo, un hospital. Se utilizan tecnologías conocidas como WLAN, GSM, UMTS o Ethernet para estos fines. Los servicios de asistencia sanitaria finales pueden ser de naturaleza centralizada, por ejemplo, el servicio de proveedor de asistencia sanitaria, el servicio de registro de asistencia sanitaria personal, o el servicio de seguridad de la asistencia sanitaria. Sin embargo, estos servicios de asistencia sanitaria también podrían distribuirse entre varias instituciones de asistencia sanitaria o compañías de seguros.

Las características técnicas de los WMS utilizados en aplicaciones médicas, así como los requisitos de funcionamiento de las MSN imponen nuevos desafíos para la definición de un sistema de seguridad, especialmente en comparación con las redes de ordenadores tradicionales o redes de sensores inalámbricas independientes estáticas.

En primer lugar, los WMS son dispositivos con recursos limitados. Por ejemplo, la plataforma MicaZ ha sido utilizado por muchas instituciones de investigación en el diseño de WMS. MicaZ está equipado con una memoria flash de programa de 128 Kbytes, una memoria RAM de 4 Kbytes. El chip de radio, el CC2420, implementa el AES en hardware y se comunica a 250 kbps. La CPU funciona a una frecuencia de reloj de 8 MHz y carece de operación de división. Por lo tanto, las soluciones de seguridad deben tener alta eficiencia energética, reducir al mínimo los requisitos de memoria, especialmente memoria RAM, y consumir una cantidad insignificante de recursos computacionales y de comunicación para evitar ataques de DoS (denegación de servicio).

Otro aspecto que impone requisitos a las aplicaciones médicas se refiere a la latencia máxima permitida en la transmisión de información médica, así como el tiempo de configuración de BSN. Por ejemplo, ECG requiere una latencia máxima de 250 mseg, y la configuración de la red debe llevarse a cabo en menos de 1 segundo. Por lo tanto, el tiempo de ejecución de los procedimientos de seguridad debe minimizarse con el fin de no restringir el funcionamiento normal de todos los días, por ejemplo, durante las visitas de un médico, y para evitar que los atacantes lanzar ataques de denegación de servicio.

Además, el sistema de seguridad debe ser escalable tanto a nivel de MSN como a nivel de WSN. Por un lado, la arquitectura de la asistencia sanitaria omnipresente debe permitir la incorporación y la integración de nuevas MSNs, por ejemplo, en una nueva residencia de ancianos, en el sistema de asistencia sanitaria omnipresente. Por otro lado, una MSN independiente puede comprender miles de WMS, por ejemplo, en un hospital. Por lo tanto, los servicios de seguridad, así como su aprovisionamiento, deben ser escalables en estos dos niveles para permitir un sistema de asistencia sanitaria verdaderamente omnipresente y seguro para un gran número de MSN y pacientes.

La movilidad de WMS con y entre los usuarios de una MSN impone requisitos adicionales sobre la asociación y configuración de BSN, así como en los enfoques de distribución de clave. En primer lugar, la asociación de BSN, que puede llevarse a cabo con mucha frecuencia, debe ser discreta, automática, palpable, segura y transparente para el personal médico, para evitar la distracción de la atención al paciente. Cada BSN puede considerarse un dominio de seguridad independiente dinámico dentro de una MSN, donde WMS pueden unirse y salir en cualquier momento, por ejemplo, un nuevo WMS de una MSN de un hospital puede unirse a un paciente, y se asociarse con su BSN. Por otro lado, la movilidad de los pacientes y cuidadores hace que una topología de MSN sea dinámica y ocasiona la segmentación de la red y las fusiones de red. Por ejemplo, la BSN de los pacientes en un hospital pueden desconectarse de la MSN y la infraestructura del hospital, por ejemplo, al ir a dar un paseo en el jardín del hospital. Situaciones como las emergencias médicas pueden requerir tratamiento inmediato por un médico. Por lo tanto, cualquier médico debe ser capaz de establecer una comunicación segura de una manera ad hoc y monitorear los signos vitales del paciente de una manera segura, impidiendo el uso de algunos protocolos de distribución de claves.

Por último, el sistema de asistencia sanitaria debe permitir la identificación única de los usuarios y BSN en diferentes MSN con el fin de vincular inequívocamente EHI de usuarios que pueda generarse en diferentes MSN por diferentes WMS.

Desafíos de seguridad

Hay tres principales desafíos de seguridad que deben abordarse para definir un sistema de seguridad integral: la distribución de claves en las MSN omnipresentes, la asociación de BSN segura, y la identificación de usuario inequívoca y única.

La DISTRIBUCIÓN DE CLAVES es la piedra angular de la seguridad tanto de las MSN independientes como de las MSN interconectadas, ya que esto define cómo los WMS reciben y manejan las claves criptográficas utilizadas para permitir los requisitos de seguridad más básicos, como la confidencialidad y la autentificación tanto intra- como inter-MSN. Hay una variedad de técnicas muy diferentes de distribución de claves en base a la clave pública, centros de confianza centralizados (en línea) o intercambio de claves. En general, la viabilidad de un enfoque u otro depende de los requisitos operativos y las restricciones técnicas de cada configuración médica específica. Por ejemplo, las claves criptográficas simétricas pueden pre-configurarse en el WMS que pertenece a una BSN estática en una pequeña MSN. Sin embargo, esta configuración es imposible en entornos altamente dinámicos, por ejemplo, hospitales, debido a la movilidad de nodo, donde la afiliación a la BSN es impredecible. La realización de las operaciones computacionalmente complejas aumenta la descarga de la batería y el retardo de las comunicaciones y podrá hacer que los protocolos de comunicación sean susceptibles a los ataques de denegación de servicio que podrían bloquear el procesamiento requerido de los datos médicos. Las implementaciones más eficientes de los sistemas de clave pública basados en criptografía de curva elíptica todavía requieren 0,81 s. para una multiplicación de un solo punto, es decir, la operación básica para establecer una clave común. Este hecho hace que estos protocolos de establecimiento de claves sean propensos a ataques de agotamiento de los recursos destinados a recursos computacionales y de energía. Por lo tanto, el uso de la criptografía de clave pública en las MSN debe reducirse al mínimo posible. El establecimiento de claves basado en un centro de confianza (TC) en línea se basa en el TC para distribuir las claves al WMS, por ejemplo, ZigBee. Este enfoque cuenta con el único punto de la naturaleza de fallo del TC y el aumento de la carga de tráfico de los nodos de la ruta del TC que drena las baterías de estos nodos. Los ataques de DoS y las colisiones de paquetes también podrían evitar que los WMS tengan éxito en el protocolo de intercambio de acuerdo de clave inicial, y por lo tanto, evitando su la transmisión de datos médicos. Además, la conectividad a un TC no puede garantizarse en muchas situaciones, como emergencias médicas y respuesta a los desastres. Por estas razones, las soluciones de criptografía de claves simétricas baratas computacionalmente que permiten un acuerdo de claves directas, tales como las funciones de hash o polinomios, son la opción preferible en MSN independientes.

ASOCIACIÓN DE BSN SEGURA se refiere a la formación de una BSN y cómo el WMS de una BSN se identifica y asocia con un usuario particular. En escenarios estáticos, en los que solo conjuntos fijos de sensores inalámbricos se comunican, la asociación de BSN se lleva a cabo solo una vez a través de un simple proceso de emparejamiento. Sin embargo, en los entornos más complejos, como en residencias de ancianos u hospitales, donde la BSN de un usuario puede consistir en conjuntos arbitrarios de WMS tomadas del conjunto de WMS de la MSN, los WMS debe estar asociados de forma segura a un paciente. Dentro del dominio de seguridad de una MSN, una BSN debe entenderse como un subdominio de seguridad completamente independiente en el que las relaciones de seguridad se manejan de manera autónoma.

El problema de la asociación de BSN ha sido recientemente abordado de diferentes maneras. Baldus et al., "Configuración fiable de redes de sensores corporales médicas", EWSN 2004, utilizó una unidad de configuración para distribuir el identificador BSN a los nodos médicos a través de infrarrojos. El enfoque BLIG (J. Andersen, y J.E. Bardram. "BLIG: Un nuevo enfoque para la identificación, agrupamiento y autorización de sensores en redes de sensores corporales ". 4th Int. Taller sobre redes de sensores corporales usables e implantables, (BSN 2007), 26-28 de marzo de 2007, Aachen, Alemania), hace uso de un nodo especial unido al cuerpo. Los otros nodos reciben el identificador de usuario cuando se ponen cerca del mismo por medio de una tecnología de comunicación de corto alcance. Falck et al. "Simplicidad Plug & Play para los sensores corporales médicos inalámbricos", Conferencia y Talleres de Salud Omnipresente, 2006, vol., n.º, pp.1-5 29 de Nov. 2006 - dic. 1, 2006, propone el uso de la tecnología de comunicación acoplada al cuerpo (BCC) para distribuir la ID de BSN y usuario. En este enfoque, cada paciente lleva un token de identificación que distribuye automáticamente la ID del paciente, y otra información de configuración, a WMS unidos al cuerpo del paciente por medio de BCC. Por lo tanto, este enfoque no requiere la intervención médica durante la configuración de la BSN. Sin embargo, los protocolos de asociación BSN seguros son necesarios ya que estos enfoques no son compatibles con los servicios de seguridad básicos ni permiten transformar una BSN en un dominio de seguridad independiente.

La identificación de usuario inequívoca y única se refiere al hecho de que un individuo puede ser atendido en diferentes MSN con diferente equipo médico como se describió anteriormente. La información médica medida debe estar vinculada de forma automática a un identificador del paciente principal reconocido en todo el sistema de asistencia sanitaria con el fin de permitir la interoperabilidad entre las MSN omnipresentes independientes. Estos identificadores deben estar regulados con el fin de garantizar la interoperabilidad entre diferentes instituciones administrativas y de asistencia sanitaria. Pueden utilizarse identificadores de sesión dinámicos para garantizar la privacidad del paciente y para identificar a un paciente de una manera diferente en función del contexto.

Una solución integrada para los tres requisitos descritos anteriormente permite el despliegue de BSN seguras y MSN, así como la seguridad integral entre WMS y servicios de asistencia sanitaria finales. El diseño de un sistema de este tipo es difícil y complejo, ya que los usuarios pueden moverse a través de diferentes organizaciones de MSN, y en algunas aplicaciones, las BSN de los usuarios pueden comprender subconjuntos de WMS arbitrariamente recogidos del conjunto de WMS de la MSN.

Requisitos adicionales de seguridad

Además del asunto de seguridad principal destinado a garantizar la configuración segura del sistema, se necesitan servicios de seguridad adicionales. Tenga en cuenta que la prestación de muchos de estos servicios de seguridad tradicionales se basa en claves criptográficas e identificadores. Vamos a proporcionar una visión general de los mismos en breve.

a) La privacidad y confidencialidad se refiere a la protección de datos, la identidad y la información de contexto para evitar que los atacantes espíen la comunicación. Por ejemplo, la confidencialidad de datos se consigue por medio de algoritmos de criptográficos, tales como el estándar criptográfico de antelación (AES).

b) Integridad de datos se refiere a la protección de datos contra la manipulación no autorizada por medio de, por ejemplo, un código de autentificación de mensajes.

c) La identificación y la autentificación se ocupa de las técnicas utilizadas para garantizar la validación de los diferentes eventos médicos, las identidades de los usuarios, y los datos intercambiados. Los identificadores deben estar regulados y estandarizados con el fin de garantizar la interoperabilidad y la identificación sin ambigüedad como lo requiere la HIPAA. Las identidades deben estar vinculados a algún material de creación de claves criptográficas con el fin de garantizar la autentificación.

d) Auditoría se refiere a las técnicas utilizadas para registrar todos los accesos a datos y es necesaria para cumplir con los requisitos de la HIPAA sobre la responsabilidad y proporcionar un registro rastreable en caso de mal uso.

e) Las técnicas de control de acceso son necesarias para autorizar el acceso a EHI del paciente y BSN. Además, hay que definir políticas de control de acceso para abordar asuntos tales como las prioridades de control de acceso y la delegación como se define en R.J. Anderson, "Un modelo de política de seguridad para los sistemas clínicos de información", sp, p. 0030, 1996 Simposio de IEEE sobre Seguridad y Privacidad, 1996; y K. Sohr, M. Drouineaud, G. Ahn. "Memoria descriptiva formal de las políticas de seguridad basadas en roles para los sistemas de información clínica" Simposio ACM sobre Informática Aplicada, 2005, Santa Fe, Nuevo México, 13 - 17 de marzo, 2005.

La seguridad y la privacidad son esenciales en el ámbito médico con el fin de cumplir con los requisitos legales, tales como HIPAA en EE.UU. o la Directiva Europea 95/46 sobre protección de datos en Europa. En este contexto, la seguridad integral entre nodos de sensores médicos (o dispositivos) y los servicios de asistencia sanitaria finales en los hospitales es un problema de suma importancia que se encuentra actualmente sin resolver. La seguridad integral debe ser independiente del conjunto de nodos de sensores usados para monitorizar a un paciente, e independiente

del servicio de asistencia sanitaria utilizado durante el ciclo de cuidados. Este requisito incluye (i) la asociación segura de la red de sensores corporales s, (ii) el almacenamiento seguro de información relacionada con la medicina en la red de sensores corporales, (iii) la inequívoca, pero al mismo tiempo privada, identificación de los pacientes en el todo el sistema, y (iv) la transmisión segura de la información del paciente entre los nodos de sensores y servicios de asistencia sanitaria.

Las tecnologías conocidas relacionadas con la técnica anterior no resuelven estos problemas:

La solicitud de patente de EE.UU. 2007/0043594 describe un sistema electrónico de suministro de asistencia sanitaria que comprende: (I) un chip controlador de NFC (comunicaciones de campo cercano; (Ii) un chip controlador de tarjeta inteligente; (Iii) un protocolo de comunicación peer-to-peer inalámbrica; etc. Aunque el objetivo de este sistema es permitir la asistencia sanitaria omnipresente, hay algunas diferencias básicas y deficiencias dentro de esta técnica anterior. En primer lugar, hay que señalar que este sistema se basa en la tecnología NFC. Es importante destacar que esta solicitud de patente no aborda los problemas de seguridad, por ejemplo, la distribución de claves, la asociación de redes de sensores corporales, la seguridad integral en la asistencia sanitaria omnipresente en absoluto. Del mismo modo, esta solicitud de patente no divulga las redes de sensores inalámbricas y redes de sensores corporales en absoluto.

DE 20008602 U divulga un sistema en el que los signos vitales del paciente, medidos por un conjunto de sensores de ECG que lleva un paciente, están vinculados a la identidad del paciente. La solicitud de patente describe un lector de tarjetas para permitir la identificación del paciente. Sin embargo, este sistema no divulga la seguridad integral y la asociación a la red de sensores corporales segura.

US 2005/10245995 A1 divulga una unidad de transmisión de datos para la comunicación inalámbrica con un implante electro-médico y un centro de adquisición y evaluación de datos. Este sistema no divulga un protocolo de seguridad integral de las redes de sensores médicos que incluye la distribución de claves en redes de sensores corporales, asociación a la red de sensores corporales, identificación de red de sensores corporales y la seguridad integral.

US 2003/10229518 A1 divulga un procedimiento para registrar las acciones de los pacientes. El sistema proporciona un equipo médico para identificar a un paciente de modo que los datos obtenidos durante el uso del equipo médico se atribuyan al paciente. Este sistema no divulga un sistema para identificar las redes de sensores corporales y habilitar la seguridad integral de las redes de sensores corporales para los sistemas médicos finales.

US 6.564.056 B1 describe un controlador que administra los dispositivos que están registrados en el controlador. Cada dispositivo se registra en el controlador mediante la inserción de una memoria en el lector de tarjetas del controlador. Las comunicaciones entre el controlador y los dispositivos están aseguradas mediante el uso de identificadores de los dispositivos como las claves criptográficas. Esta aplicación no divulga un lector de tarjetas que identifica y registra los dispositivos de la red de sensores corporales, sino que identifica el usuario de la red de sensores corporales.

US 200210188473 describe un sistema que incluye la identificación del paciente y permite que el usuario tenga acceso a la historia médica del paciente. El sistema está basado en una tarjeta inteligente. Este sistema no tiene en cuenta las redes de sensores inalámbricas y las redes de sensores corporales, la identificación de la red de sensores corporales, identificación de los nodos de sensores, asociación de redes de sensores corporales seguras, y seguridad integral entre nodos de sensores y sistemas médicos finales.

WO2007 / 149850 A2 describe un procedimiento de distribución de claves que permite a cualquier par de dispositivos en un hospital acordar una clave común de una manera distribuida. De esta manera, esta solicitud de patente garantiza servicios básicos de seguridad entre nodos de sensores o entre un nodo de sensores y un monitor de cabecera. Sin embargo, la brecha de seguridad importante de la seguridad integral está aún sin resolver.

WO2008/014432 A2 describe un procedimiento para permitir la identificación del paciente en base a las comunicaciones acopladas al cuerpo (BCC). En esta solicitud de patente, cada paciente lleva una etiqueta de comunicaciones acoplado al cuerpo. Cuando un paciente quiere hacer uso de un dispositivo médico específico o similar, el dispositivo médico se comunica con la etiqueta de comunicaciones acoplada al cuerpo por medio de comunicaciones acopladas al cuerpo para recibir el ID de paciente. De esta manera el dispositivo médico puede hacer uso de la información de identificación del paciente para personalizar sus mediciones o para adjuntar la identificación del paciente a los signos vitales medidos antes de enviarlos a un médico. Aunque este enfoque permite la identificación de los pacientes de una manera muy simple, las amenazas a la seguridad en el sistema no se tienen en cuenta. Por ejemplo, un intruso, Bob, podría robar la etiqueta de Alice y leer la información de identificación de Alice. Posteriormente, Bob podría hacerse pasar por Alice o incluso tener acceso a la información médica personal de Alice. Esta solicitud se refiere al problema de la seguridad integral entre nodos de la red de sensores corporales y servicios de asistencia sanitaria finales. Con este fin, la presente solicitud resuelve los siguientes temas de seguridad:

1. La disposición segura de una red de sensores corporales - en el sentido de que todas las comunicaciones entre todos los dispositivos de una red de sensores corporales son seguras con respecto a la autentificación y la confidencialidad;

2. La identificación inequívoca del paciente - en el sentido de que un paciente se identifica de forma inequívoca en todo el sistema, incluyendo redes de sensores corporales, servicios de seguridad finales, etc.; y

3. El almacenamiento seguro de información médica, de manera que solo personal autorizado pueda tener acceso a ella.

Sumario de la invención

El sistema seguro integral de asistencia sanitaria al paciente se basa en el uso de PSM de administrador de seguridad personal en una BSN de red de sensores corporales que lleva la información de un paciente, por ejemplo, información médica o relacionada con el identificador, de una manera segura. El administrador de seguridad personal puede comunicarse de una manera segura con el resto de los nodos de sensores WMS dentro de la red de sensores corporales, por ejemplo, los nodos de sensores médicos o dispositivos de monitorización, y transmitir identificadores de pacientes reales, que son reconocidos en todo el sistema, incluyendo los sistemas finales, por medio de comunicaciones acopladas al cuerpo (BCC). BCC es la tecnología preferida, pero otras, como comunicaciones de campo cercano (NFC) o similares, se podrían utilizar también. Además, el administrador de seguridad personal también lleva la información de seguridad incluida la identificación del paciente, clave pública, etc., que permite al administrador de seguridad personal para autentificar la identidad del paciente y activar la seguridad integral con el sistema final. La seguridad entre los sistemas PSM y finales podría estar basada en una infraestructura de clave pública o basada en terceros de confianza (como el protocolo de autentificación de red informática Kerberos) o combinaciones adicionales.

Además de las tecnologías mencionadas anteriormente que se utilizan para la transmisión de EHI de los usuarios, el sistema de seguridad integral hace uso de dos tecnologías adicionales, a saber, la comunicación acoplada al cuerpo BCC y las tarjetas inteligentes, para la identificación segura y transparente y la formación de una BSN, así como para el almacenamiento seguro de material de seguridad y EHI. La BCC es una comunicación en el cuerpo de baja energía que utiliza el cuerpo humano como capa de red física para la transmisión de datos entre los dispositivos unidos directamente al cuerpo de un paciente. Esta tecnología ahorra energía y espectro y mejora el nivel de seguridad en comparación con la comunicación inalámbrica tradicional debido a los bajos requisitos de energía y la naturaleza de comunicación en el cuerpo que hace que sea más difícil escuchar a escondidas las comunicaciones. Por lo tanto, puede utilizarse por WMS que pertenezcan al mismo paciente para el intercambio de datos sensibles, la activación de la asociación de BSN, es decir, la asignación de un WMS a una BSN, o el intercambio de datos médicos. La tecnología de tarjetas inteligentes proporciona un medio seguro para almacenar información crítica de una manera segura, así como la autentificación de usuario. Una tarjeta inteligente proporciona las capacidades criptográficas para permitir la autentificación y el almacenamiento seguro de los datos.

La combinación de BCC y la tecnología de tarjeta inteligente proporciona un sólido mecanismo de autentificación e identificación. Las buenas características de seguridad de una tarjeta inteligente, como el control de acceso basado en PIN o algoritmos criptográficos integrados permiten el almacenamiento seguro de información privada, por ejemplo, contraseñas. Las propiedades de comunicación privadas inherentes de BCC proporcionan un medio de transmisión seguro que hace difícil espiar. Por ejemplo, podemos imaginar un usuario que lleva un token de identificación con capacidades de tarjetas inteligentes y BCC. El usuario puede almacenar en la tarjeta inteligente información como contraseñas o datos privados. Esta información solo puede ser recuperada de la tarjeta inteligente, por ejemplo, a través de un enlace BCC después de la identificación y autentificación con éxito.

Una tarjeta de asistencia sanitaria HCC, por ejemplo, una tarjeta inteligente, puede conectarse a un administrador de seguridad personal PSM para proporcionar una conexión entre la red de sensores corporales y dominios de seguridad finales que resuelve los problemas de seguridad anteriores. El administrador de seguridad personal lleva la información del paciente, por ejemplo, nombre, información médica, contraseñas, etc. en una tarjeta de asistencia sanitaria de una manera segura que

i) incluye funcionalidades que permitan la asociación segura de nodos de red de sensores corporales y transmite identificadores de pacientes reguladas que son reconocidos en todo el sistema de asistencia sanitaria por medio de comunicación de comunicaciones acopladas al cuerpo BCC de una forma segura como se describe anteriormente. Solo los dispositivos médicos inalámbricos asociados a la misma BSN y contar con las credenciales necesarias permiten recuperar la información privada de la HCC conectada en el PSM a través del enlace BCC, y

ii) lleva la información del paciente, por ejemplo, identificación del paciente, la clave pública del paciente, etc., que permite al administrador de seguridad personal autentificar la identidad del paciente y habilitar la seguridad integral entre nodos de la red de sensores corporales y servicios de asistencia sanitaria. El administrador de seguridad personal puede implementarse en un nodo con interfaces de comunicación inalámbricos y acoplados del cuerpo y

puede incluir un módulo de seguridad para habilitar funcionalidades de seguridad en las comunicaciones de red de sensores inter- e intra-corporales.

Algunas de las funcionalidades de seguridad están separadas físicamente de otros componentes dentro del sistema y se pueden almacenar en la tarjeta de asistencia sanitaria, aumentando tanto la flexibilidad como el valor del sistema.

Los principios descritos en esta invención se pueden aplicar a los dispositivos y redes de sensores corporales médicos para activar la seguridad integral en los sistemas de monitoreo de pacientes omnipresentes, como el ciclo de cuidados.

Una red de sensores corporales BSN es una red inalámbrica particular, ad hoc compuesta de sensores inalámbricos WMS adaptados para unirse al cuerpo de un paciente y también puede incluir un número de dispositivos médicos inalámbricos en estrecha proximidad, como se muestra en la fig. 1. Los nodos de sensores inalámbricos, por ejemplo, los sensores médicos inalámbricos WMS, miden los signos vitales de un paciente y los transmiten a un monitor de PDA o a un monitor al lado de la cama que los muestra y los envía a una unidad de almacenamiento central o similar.

Este sistema de seguridad integral supera los retos anteriores y permite el acceso eficaz y seguro a los datos médicos personales en redes de sensores médicos omnipresentes. El sistema combina las tecnologías existentes, tales como la comunicación acoplada al cuerpo y el concepto de la tarjeta de asistencia sanitaria digital, con soluciones de seguridad distribuidas para permitir una asociación de red de sensores corporales segura, un acuerdo de claves distribuido eficiente y control de acceso en redes de sensores corporales, la identificación inequívoca del paciente, y la seguridad integral a través de los escenarios de asistencia sanitaria omnipresentes. Este sistema proporciona la facilidad de uso, rendimiento y seguridad, que son especialmente adecuados para sensores médicos inalámbricos con recursos limitados.

Es un objeto de la presente invención proporcionar un aparato y un procedimiento que proporcionen comunicaciones seguras integrales entre todas las partes de una red de comunicaciones para la asistencia sanitaria, desde los sensores médicos inalámbricos individuales de una red de sensores corporales a los servicios finales.

Según un primer aspecto de la presente invención, un sistema seguro integral de asistencia sanitaria al paciente incluye:

- uno o más sensores médicos inalámbricos adaptados para acoplarse al cuerpo de un paciente y en comunicación entre sí formando una red de sensores corporales dentro de una red de sensores médicos inalámbrica que incluye una o más redes de sensores corporales;

- medios de creación de claves λ seguras incorporados en cada uno de dichos sensores médicos inalámbricos para habilitar las comunicaciones seguras entre dichos sensores médicos inalámbricos, y

- un administrador de seguridad personal dentro de la red de sensores corporales y en comunicación con dichos uno o más sensores médicos inalámbricos dentro de dicha red de sensores corporales, con dicho administrador de seguridad personal proporcionando comunicaciones seguras con los servicios finales y proporcionando relaciones de seguridad dentro de dicha red de sensores corporales por medio de dichos medios de creación de claves λ seguras,

en el que dichos medios de creación de claves λ seguras son tales que una coalición de no más de λ sensores médicos inalámbricos comprometidos oculta, por ejemplo, no revela nada, acerca de una tecla de pares entre dos sensores médicos no comprometidos inalámbricas y proporciona una capacidad de recuperación perfecta para el compromiso de nodos hasta λ +1 sensores médicos inalámbricos han sido comprometidos.

La sensores médicos y administrador de seguridad personal inalámbrica pueden adaptarse para comunicarse por medio de comunicaciones acopladas al cuerpo.

El sistema puede incluir además una tarjeta de asistencia sanitaria conectada al administrador de seguridad personal, en el que la tarjeta de asistencia sanitaria incluye información para la identificación del usuario inequívoca y la información de seguridad para la comunicación segura con los servicios finales de la asistencia sanitaria, en la que el administrador de seguridad personal incluye un certificado emitido por un centro de confianza a nivel local, y en el que el sistema está adaptado para ejecutar un protocolo de seguridad para la auditoría, control de acceso y protección de la privacidad, y la autentificación mutua del administrador de seguridad personal con la tarjeta de asistencia sanitaria.

La información de la red de sensores corporales puede estar vinculada a la identidad del paciente, en la que dicha tarjeta de asistencia sanitaria del paciente HCC y dicho administrador de seguridad personal PSM forman un

administrador de seguridad personal extendido PSMx, ver fig. 2, para conectar una serie de dominios de seguridad de redes de sensores médicos inalámbricos a un sistema de asistencia sanitaria omnipresente. El administrador de seguridad personal extendido puede adaptarse para:

- almacenar el certificado expedido por el centro de confianza a nivel local,

- almacenar los medios de creación de claves λ para establecer una comunicación de seguridad integral emitida por los servicios de asistencia sanitaria centralizados y

- aplicar el protocolo de seguridad para habilitar la autentificación mutua del administrador de seguridad personal extendido y la tarjeta de asistencia sanitaria, seguridad final, auditoría y gestión integral de las políticas de privacidad y control de acceso de contexto.

El administrador de seguridad personal extendido puede adaptarse para autentificar el administrador de seguridad personal del paciente y de la tarjeta de asistencia sanitaria del paciente cuando este se une a la red de sensores médicos.

El administrador de seguridad personal puede incluir un lector de tarjetas inteligentes adaptado para recibir la tarjeta de asistencia sanitaria, y en el que la tarjeta de asistencia sanitaria puede incluir información de identificación individual y/o información médica y/o material de seguridad y/o políticas de seguridad.

El administrador de seguridad personal puede incluir un nombre de usuario, identificador, materiales de seguridad, registros médicos o políticas de control de acceso para diferentes redes de sensores médicos.

El administrador de seguridad personal extendido puede incluir la identificación de un usuario global, red de área del paciente y la información de asistencia sanitaria electrónica individual EHI. La información de asistencia sanitaria electrónica EHI puede provenir de la red de área de paciente.

La información de seguridad almacenada en la asistencia sanitaria puede proporcionarse para la identificación y autentificación del usuario y para actuar como un puente entre la red de sensores corporales del paciente y los servicios de asistencia sanitaria centralizados o finales. La red de sensores corporales puede ser la misma que la red de área de paciente.

El administrador de seguridad personal extendido puede ser un teléfono móvil con una ranura de tarjeta inteligente adicional para la tarjeta de asistencia sanitaria.

El sistema de asistencia sanitaria integral del paciente seguro integral puede incluir además un dominio seguro autónomo formado por el sensor médico inalámbrico asociado con una red de área de paciente, en el que el administrador de seguridad personal extendido es el centro de confianza de la red de área de paciente y está adaptado para controlar la asociación o revocación segura de los miembros de la red de área de paciente.

El administrador de seguridad personal extendido y los sensores médicos inalámbricos se pueden adaptar para el almacenamiento seguro de información y las acciones llevadas a cabo en la red de sensores corporales de la tarjeta de asistencia sanitaria del paciente, incluso si se pierde la conexión con el centro de confianza de la red de sensores médicos intercambiada.

Según un segundo aspecto de la presente invención, un procedimiento para la comunicación de asistencia sanitaria con el paciente integral segura en un sistema de asistencia sanitaria integral del paciente incluye los pasos de: almacenar un certificado expedido por un centro de confianza de la red local de sensores médicos en el administrador de seguridad personal; almacenar los medios de seguridad en el administrador de seguridad personal para establecer una comunicación de seguridad integral emitida por los servicios de asistencia sanitaria centralizados; e implementar un protocolo de seguridad para habilitar la autentificación mutua del administrador de seguridad personal y una tarjeta de asistencia sanitaria, seguridad integral, auditoría, y/o la gestión de las políticas de privacidad de control de acceso de contexto.

Según un tercer aspecto de la presente invención, un administrador de seguridad personal para un sistema de asistencia sanitaria integral del paciente seguro, en el que el administrador de seguridad personal se encuentra dentro de una red de sensores corporales y en comunicación con uno o más sensores médicos inalámbricos dentro de la red de sensores corporales, en el que el administrador de seguridad personal proporciona comunicaciones seguras con servicios de finales y proporciona relaciones de seguridad dentro de la red de sensores corporales por medio de medios de creación de claves λ seguras, donde uno o más sensores médicos inalámbricos están adaptados para acoplarse al cuerpo de un paciente y en comunicación entre sí para formar la red de sensores corporales dentro de una red de sensores médicos inalámbricos que incluye una o más redes de sensores corporales; medios de creación de claves λ seguras incorporados en cada uno de los sensores médicos inalámbricos para habilitar las comunicaciones seguras entre los sensores médicos inalámbricos, y en el que los

medios de creación de claves λ seguras son tales que una coalición de no más de λ sensores médicos inalámbricos comprometidos oculta, por ejemplo, no revela nada, acerca de una clave de pares entre dos sensores médicos inalámbricos no comprometidos y proporciona la capacidad de recuperación perfecta al compromiso de nodos hasta que λ+1 sensores médicos inalámbricos han sido comprometidos.

Un establecimiento de claves λ seguras se refiere a un protocolo de intercambio de establecimiento de claves que presenta la propiedad de λ seguras. Un ejemplo típico consiste en un polinomio de dos variables simétrico f (x, y) de grado λ sobre un campo finito Fq donde q es lo suficientemente grande para dar cabida a una clave criptográfica. Este polinomio es el material de creación de claves de de origen en el sistema de λ seguras. A partir de este material de creación de claves, la autoridad central del sistema puede obtener cuota de material de creación de claves λ seguras. Cada entidad (por ejemplo, el nodo de sensores) en el sistema llevará una cuota de material de creación de claves λ seguras. Por ejemplo, a partir del material de creación de claves de origen anterior f (x, y) una entidad con identificador ID llevaría el material de creación de claves λ seguras f (ID, y), es decir, el polinomio de dos variables originales evaluado en x = ID.

Cualquier par de entidades en el sistema, por ejemplo, ID_A y ID_B que lleve f (ID_A, y) yf (ID_B, y), respectivamente, puede ponerse de acuerdo sobre una clave común de pares de la siguiente manera:

- intercambian sus identificadores

- explotan a sus materiales de creación de claves alfa seguras junto con los identificadores. En este caso concreto, la entidad A toma el material clave de creación de claves alfa seguras (f (ID_A, y)) y lo evalúa en y= ID_B, es decir, el identificador de la otra parte. El resultado es f (ID_A, ID_B).

- La entidad B hace exactamente lo mismo con su cuota de material de creación de claves alfa seguras y el identificador de la otra parte. El resultado es f (ID_B, ID_A).

- Dado que el material de creación de claves de origen es un polinomio simétrico, el resultado obtenido por ambas entidades es idéntico, es decir,

f (ID_A, ID_B) = f (ID_B, ID_A) = K. K es la clave común compartida por ambas partes. Esta clave se utiliza para proporcionar más servicios de seguridad.

El sistema puede hacer uso de otros protocolos de establecimiento de claves λ seguras, es decir, otros protocolos criptográficos con la propiedad λ segura. También puede basarse en polinomios, pero con otras características para mejorar, por ejemplo, su capacidad de recuperación en función de los modelos de despliegue, proporcionando más servicios de seguridad más avanzados como el control de acceso o el rendimiento más eficiente. Por ejemplo, se ha propuesto la utilización de modelos de despliegue con una estructura jerárquica (múltiple) en el ámbito médico. Estos esquemas ofrecen un nivel de seguridad más alto, ya que, por ejemplo, introducen una mayor cantidad de material de creación de claves en el sistema o una clave de pares entre dos entidades se calcula como una combinación de las claves generadas a partir de varios dominios de seguridad de λ seguras independientes. Los esquemas de λ seguras utilizados en el sistema de seguridad integral se pueden adaptar también para proporcionar otros servicios de seguridad como el control de acceso o identificación (privada). Esto se logra mediante la vinculación del material de creación claves λ seguras con información de identificación o funciones de control de acceso. Los esquemas de λ seguras también pueden adaptarse para minimizar los requisitos de cálculo, por ejemplo, mediante el uso de técnicas combinatorias basadas en planos proyectivos finitos, técnicas de clave de segmentación, o técnicas de segmentación de identificador.

El uso de técnicas de λ seguras permite que dos entidades se pongan de acuerdo sobre una clave por pares, es decir, una clave compartida entre dos entidades. Por ejemplo, imaginemos dos personas, Alice y Bob, intercambiando la clave simétrica, K. Si Alice quiere enviar un mensaje a Bob de manera confidencial, Alice utiliza un algoritmo criptográfico simétrico para encriptar el mensaje con la clave K. Bob es capaz de desencriptarlo con la misma clave. En este caso, esta clave es por parejas, ya que solo es compartida por Alice y Bob.

Se entenderá que el procedimiento reivindicado tiene modos de realización preferidos, similares y/o idénticos a los del aparato y según lo definido en las reivindicaciones dependientes.

Breve descripción de los dibujos

Estos y otros aspectos de la invención serán evidentes a partir de, y se esclarecerán con referencia a, el (los) modo(s) de realización descritos a continuación. En los siguientes dibujos:

La figura 1 ilustra una red de sensores corporales para un sistema seguro integral de asistencia sanitaria al paciente según un modo de realización de la presente invención;

La figura 2 ilustra los componentes de un sistema seguro integral de asistencia sanitaria al paciente según un modo de realización de la presente invención;

La figura 3 ilustra las disposiciones de seguridad dentro de un administrador de seguridad personal para un sistema seguro integral de asistencia sanitaria al paciente según un modo de realización de la presente invención;

Las figs. 4A-4C ilustran las disposiciones de protocolo de seguridad dentro de una red de sensores corporales según un modo de realización de la presente invención;

Las figs. 5A-5E ilustran las disposiciones de un protocolo de seguridad para la seguridad integral dentro de un sistema de asistencia sanitaria del paciente según un modo de realización de la presente invención;

La figura 6 ilustra una instalación que incorpora el sistema de asistencia sanitaria del paciente seguro integral según un modo de realización de la presente invención;

La figura 7 ilustra los enlaces de comunicaciones para un sistema seguro integral de asistencia sanitaria al paciente según un modo de realización de la presente invención;

La figura 8 representa la información transportada por un sensor médico inalámbrico en una red de sensores médicos en particular según un modo de realización de la presente invención;

La figura 9 ilustra el establecimiento eficiente de un canal de comunicación seguro entre dos sensores médicos inalámbricos que pertenecen a la misma red de sensor médico según un modo de realización de la presente invención;

La figura 10 ilustra el procedimiento para permitir la asociación de la red de sensores corporales segura entre un sensor médico inalámbrico y el administrador de seguridad personal según un modo de realización de la invención;

La figura 11 ilustra la estructura del administrador de seguridad personal extendido según un modo de realización de la invención;

La figura 12 ilustra las comunicaciones entre el administrador de seguridad personal extendido y la autoridad de certificación de la asistencia sanitaria central de los servicios de asistencia sanitaria finales según un modo de realización de la invención;

La figura 13 proporciona una tabla que ilustra la comparación de rendimiento de algunas primitivas de seguridad en MICAz y uPD789828 según un modo de realización de la invención; y

La figura 14 proporciona una tabla que ilustra las asignaciones de recursos de memoria en los dominios sub-seguros de un establecimiento de claves λ seguras multidimensional según un modo de realización de la invención.

Descripción detallada de la invención

El sistema seguro integral de asistencia sanitaria al paciente se basa en el uso de un administrador de seguridad personal PSM o un controlador de BSN de red de sensores corporales que lleva la información de un paciente, por ejemplo, el identificador, la información relacionada médico, de una manera segura. El administrador de seguridad personal puede comunicarse de una manera segura con el resto de los nodos de sensores dentro de la red de sensores corporales, por ejemplo, los nodos de sensores médicos o dispositivos de monitorización, y transmitir identificadores de pacientes reales, que son reconocidos en todo el sistema, incluyendo los sistemas finales, por medio de BCC de comunicaciones acopladas al cuerpo. Además, el administrador de seguridad personal también lleva la información, que incluye información de identificación del paciente, clave pública, etc, que permite al administrador de seguridad personal autentificar la identidad del paciente y activar la seguridad integral con el sistema final.

La arquitectura de seguridad comprende varios elementos físicos, como se muestra en las figs. 1 y 2: Los nodos de sensores, por ejemplo, WMS, se utilizan para controlar los signos vitales del paciente, y pueden dividirse en dos o más tipos diferentes. Por un lado, algunos nodos de sensores médicos se utilizan para detectar y transmitir los signos vitales de un paciente. Por otro lado, los dispositivos de monitorización, tales como PDAs o monitores, se comunican con los nodos de sensores médicos y muestran signos vitales del paciente. Las comunicaciones pueden llevarse a cabo por medio de una interfaz inalámbrica. Además, algunos nodos de sensores pueden tener comunicaciones o capacidades inductivas acopladas al cuerpo.

Los servicios de asistencia sanitaria son servicios finales BS, por ejemplo, un HPS de servicio de proveedor de asistencia sanitaria, un servicio de registro de asistencia sanitaria personal PHRS y/o un proveedor de seguridad de la asistencia sanitaria HSP. Estos servicios administran, almacenar y proporcionar acceso a los datos médicos del

paciente, de manera que los datos médicos están disponibles 24/7.

El administrador de seguridad personal organiza las relaciones de seguridad entre los nodos de sensores médicos, los dispositivos de control y los servicios de asistencia sanitaria. Por lo tanto, el administrador de seguridad personal juega un papel de especial importancia. Tenga en cuenta que la infraestructura de seguridad podría no incluir todos estos elementos físicos, es decir, algunos de los servicios de seguridad o dispositivos de monitorización podrían no estar presentes.

En la fig. 2, la comunicación con los servicios de asistencia sanitaria se indica mediante una línea trazada; la comunicación BCC o comunicación inductiva se indica mediante una línea discontinua, y la comunicación inalámbrica se indica mediante una línea de puntos.

Elementos criptográficos implicados en la arquitectura de seguridad

La arquitectura de seguridad requiere diferentes elementos que se describen a continuación. La mayoría de estos elementos y funcionalidades son implementadas en el administrador de seguridad personal ya que se utiliza como un enlace entre los nodos de los sensores y los servicios de asistencia sanitaria (véase la fig. 3) desde el punto de vista de la seguridad.

1. Se utiliza un PIN de activación para autentificar al usuario antes de su uso. Esta funcionalidad es específica para el administrador de seguridad personal PSM y se utiliza para evitar que personas no autorizadas tengan acceso al administrador de la seguridad personal.

2. El material de creación de claves KM permite comunicaciones seguras entre los nodos de sensores, o entre los nodos de sensores y el administrador de seguridad personal.

3. Se utiliza la información de identificación del paciente (identidad digital) para identificar un paciente y comprende:

a. Un identificador de paciente;

b. Información criptográfica relacionada con el identificador del paciente. Un posible modo de realización es el uso de un par de claves públicas / privadas unidas a la identidad del paciente. La autenticidad y la validez de estas claves se basa en una infraestructura de clave pública. Otro modo de realización sería el uso de un tercero de confianza. En este caso, un secreto simétrico único vinculado al paciente se utilizaría para establecer más relaciones de seguridad basados en el centro de confianza en línea.

c. El controlador de identidad digital (administrador de identidad digital) se puede utilizar para manejar la divulgación de la identidad digital del paciente. La validez de identificador del paciente y la información criptográfica relacionada, por ejemplo, la clave pública, se basa en un servidor de seguridad de la asistencia sanitaria que gestiona las relaciones de seguridad en todo el sistema. Por lo tanto, estas funcionalidades pueden implementarse tanto en el administrador de seguridad personal como en el servidor de seguridad de asistencia sanitaria. El controlador de la identidad digital reside en el administrador de seguridad personal.

Dependiendo del modo de realización particular, algunos de los elementos anteriores no pueden estar presentes. Diferentes modos de realización de la invención pueden requerir otros elementos de identificación, por ejemplo, técnicas de identificación biométrica.

4. El administrador de seguridad personal también puede tener una memoria MEM seguro para permitir el almacenamiento seguro de información, tal como: información médica relacionada, identidad digital de un paciente, derechos de control de acceso, contraseñas del paciente, etc ... La memoria segura MEM puede estar integrada en el propio PSM o en la HCC.

Las funcionalidades del administrador de seguridad personal se representan en detalle en la fig. 3. Varios modos de realización pueden incluir una serie de características únicas, por ejemplo, el administrador de seguridad personal PSM, que puede activarse solo después de la entrada con éxito de PIN del usuario; el administrador de seguridad personal puede tener algo de inteligencia, es decir, un bloque lógico, incluyendo la descripción de los protocolos de seguridad; el administrador de seguridad personal puede incluir material de creación de claves KM para permitir la comunicación segura con nodos de sensores; el administrador de seguridad personal puede almacenar información relacionada con el paciente, incluyendo: identidad digital del paciente, información médica, derechos de control de acceso o contraseñas; y el material de creación de claves y la lógica se pueden integrar en el administrador de seguridad personal; Sin embargo, la información relacionada con el paciente se puede almacenar en una tarjeta inteligente, por ejemplo, una tarjeta de asistencia sanitaria HCC. De esta manera, el mismo administrador de seguridad personal puede ser utilizado por diferentes pacientes mediante la sustitución de la asistencia sanitaria del paciente en el administrador de seguridad personal.

Funcionalidades de la arquitectura de seguridad

A continuación, se describe cómo el administrador de seguridad personal explota primitivas de seguridad anteriores para gestionar las relaciones de seguridad entre los nodos de sensores y los servicios de asistencia sanitaria. Algunas de estas funcionalidades y relaciones entre los diferentes elementos físicos se ilustran en las figs. 4 y 5.

1. Autentificación del usuario - antes de activar un administrador de seguridad personal, un usuario debe autentificarse a sí mismo por medio de un PIN de usuario. El PIN se introduce por medio de una interfaz de usuario (UI) o similar. Esto se puede implementar fácilmente si el PSM del controlador de red de sensores corporales se implementa en un teléfono móvil o similar. El resto de funcionalidades del controlador de red de sensores corporales puede ser operativo solo después de la autentificación de usuario exitosa. Dependiendo del modo de realización, la activación del PSM podría ser solo posible si la HCC está conectado, ya que la HCC implementa las funcionalidades de autentificación de usuario.

2. Fije la configuración automática de una red de sensores corporales - después de la activación, el administrador de seguridad personal puede utilizarse para configurar una red de sensores corporales de una manera segura. Con este fin, cuando un paciente llega a un hospital o similar, el paciente puede recibir un administrador de seguridad personal con las funcionalidades descritas anteriormente. Identificadores de los médicos, enfermeras, etc., que tienen derechos de acceso a la red de sensores corporales del paciente también pueden cargarse durante el ingreso. Además, la información relacionada con el paciente, por ejemplo, identificadores, información médica, pueden cargarse manualmente o desde el servidor del hospital. En este caso, el administrador de seguridad personal puede implementar todas las funcionalidades representadas en la fig. 3 en un único dispositivo.

Además, el administrador de seguridad personal puede incluir un lector de tarjetas para las tarjetas de asistencia sanitaria, como una tarjeta inteligente. En este caso, toda la información médica de un paciente, por ejemplo, la identidad digital del paciente, la información médica relacionada, las claves pública y privada, las contraseñas, etc, se pueden almacenar en la tarjeta inteligente HCC. Se puede acceder a esta información solo después de insertar la tarjeta de asistencia sanitaria del paciente en el administrador de seguridad personal. Parte de esta información puede estar siempre disponible, mientras que el acceso a otra información podría requerir diferentes niveles de autorización, por ejemplo, diferentes números PIN. Una vez que el paciente lleva su administrador de seguridad personal, puede ser atendido. Con este fin, los médicos pueden unir varios nodos de sensores, por ejemplo, ECG, $Sp0_{2,}$ a su cuerpo, así como un dispositivo de monitorización. Para asociar los nodos de sensores y dispositivos de monitorización a la red de sensores corporales del paciente, el médico puede hacer uso del administrador de seguridad personal como se describe en las figs. 4 y 5. Esta asociación entre el administrador de seguridad personal y la red de sensores corporales puede hacer uso de las comunicaciones acoplada cuerpo BCC, comunicaciones inductivas, por ejemplo, comunicaciones de campo cercano, o similares. El uso de BCC tiene ventajas inherentes, ya que solo los dispositivos conectados al mismo cuerpo pueden comunicarse entre sí. Además de las características de asociación descritas en las figs. 4 y 5, el mecanismo descrito es seguro debido a los siguientes aspectos específicos:

Fig. 4A - El administrador de seguridad personal PSM y los nodos de sensores WMS utilizan el material de creación de claves KM para ponerse de acuerdo sobre un secreto común y autentificarse entre sí. De esta manera, el administrador de seguridad personal garantiza que solo a las PDA de dispositivos médicos autentificados se les permite unirse a la red de sensores corporales del paciente. Las políticas de control de acceso almacenadas en el PSM (o HCC conectado al PSM) también podrían utilizarse para decidir si un nodo de sensores está autorizado para unirse a la BSN o no.

Fig..4B - El administrador de seguridad personal puede acceder a información relacionada con la del paciente, incluyendo el identificador o el registro personal de salud. Por lo tanto, el administrador de seguridad personal hace uso de información real del paciente para identificar la red de sensores corporales de una forma inequívoca y simplifica el ciclo de atención. En particular, el administrador de seguridad personal puede

(1) obtener un identificador temporal del paciente (ID del paciente) para el paciente utilizado para identificar la red de sensores corporales. Los identificadores temporales de pacientes se cambian periódicamente para evitar la esfera de la privacidad del usuario y evitar el seguimiento,

(2) establecer una clave de red BSN K que se utiliza para las comunicaciones dentro del dominio de seguridad de BSN. Toda la comunicación entre los miembros de BSN podría asegurarse en base a esta clave que permite la emisión.

(3) transmitir la información del paciente (en respuesta a una solicitud) a los nodos de sensores médicos de una manera segura sobre la base del material de creación de claves. La información transmitida puede incluir el identificador temporal del paciente o los identificadores de los médicos, enfermeras u otra PDA de personal que tenga acceso a la información médica (véase la figura 4B).

Fig. 4C - Por último, los nodos de sensores médicos pueden transmitir señales vitales del paciente al dispositivo de control de una manera segura mediante el uso de la clave K, que fue distribuida por el administrador de seguridad personal previamente, para habilitar los servicios de seguridad básicos.

3. La identificación del paciente inequívoca y el acceso a servicios de asistencia sanitaria finales representa un problema para los sistemas de la técnica anterior, ya que es difícil conectar un identificador de paciente temporal con los signos vitales medidos por un conjunto aleatorio de nodos de sensores a tales sistemas finales, por ejemplo, el registro de salud personal almacenado en un servidor.

Esta invención resuelve este problema, ya que el administrador de seguridad personal actúa como la relación de seguridad entre los nodos de sensores y los sistemas finales. Por una parte, un administrador de seguridad personal tiene material de creación de claves que permite comunicaciones seguras con los nodos de sensores. Por otro lado, el administrador de seguridad personal también puede tener la información necesaria para identificar a un paciente. Esta información puede cargarse durante el ingreso del paciente o después de conectar la tarjeta de asistencia sanitaria del paciente en el lector de administrador de seguridad personal.

Las figs. 5A-5E representan el protocolo llevado a cabo por los nodos de sensores, el administrador de seguridad personal y los sistemas finales para lograr la seguridad integral y la identificación inequívoca del paciente independientemente del conjunto de nodos de sensores que puedan ser usados para monitorear a un paciente. La figura 5A ilustra la conexión del administrador de seguridad personal a un proveedor de seguridad de asistencia sanitaria HSP para autentificar la identidad del paciente en base a la clave pública almacenada en la memoria del administrador de seguridad personal. La figura 5B representa la negociación de diferentes parámetros de seguridad, por ejemplo, una clave simétrica K que se puede utilizar para activar la seguridad integral. Después, las figs. 5C y 5D ilustran la asociación segura de los nodos de sensores a la red de sensores corporales del paciente, como se describe anteriormente, y entre la HSP y la BS. Finalmente, la fig. 5E ilustra cómo los signos vitales del paciente no solo se envían a las PDA de los dispositivos de monitorización, sino también a servicios de asistencia sanitaria de una manera segura.

4. Además de los problemas de funcionamiento que se detallan anteriormente, la arquitectura de seguridad puede permitir otros servicios de seguridad, por ejemplo:

Memoria segura - que puede ser utilizada para almacenar información confidencial como contraseñas o información relacionada con la medicina. El acceso a esta información puede estar restringido a usuarios autorizados. Son posibles diferentes niveles de autorización a través de diferentes números PIN. Un usuario que lleva un administrador de seguridad personal puede hacer uso del mismo para almacenar contraseñas de forma segura.

Conexión segura - puede ser utilizada por un usuario que lleva un PSM con capacidades BCC. Por ejemplo, imaginemos que el usuario desea comprobar su registro de asistencia sanitaria por internet. La información de acceso (por ejemplo, nombre de usuario + contraseña) se almacena en el PSM. El ordenador personal utilizado para consultar el registro sanitario puede incorporar una interfaz de BCC. Cuando el PC activa la BCC, el PSM puede autentificar el PC en base al material de creación de claves distribuido. A continuación, el usuario puede comprobar su registro de asistencia sanitaria sin introducir manualmente su nombre de usuario y contraseña. Esta información, que se almacena en el PSM, se transmite directamente al PC a través de la BCC. El mismo enfoque podría ser utilizado para acceder al correo electrónico personal, entrar en la casa, etc.

Identidad digital - Un usuario puede hacer uso de un administrador de seguridad personal para fines de identificación, y por lo tanto, el módulo de seguridad implementa un sub-módulo. En general, la identidad digital de un paciente o persona puede estar vinculada a una clave pública / privada.

Control de la red - El administrador de seguridad personal puede utilizarse para almacenar información útil, como:

i. nodos de sensores que comprenden la red de sensores corporales;

ii. dispositivos de monitorización que monitorizan los signos vitales del paciente;

iii. otros eventos que se producen durante la monitorización del paciente tales como el comportamiento inusual de los nodos de sensores. Esta información puede utilizarse para detectar los nodos de sensores defectuosos o comprometidos. En tal caso, el dispositivo comprometido debe retirarse de la BSN y la información de la BSN / el usuario como el identificador o la clave de red de BSN K debe actualizarse con el fin de proteger la privacidad del usuario.

Distribución de claves en las MSN omnipresentes

La distribución de claves es fundamental para activar la seguridad integral. Sin embargo, la elección del mejor enfoque de distribución clave depende de las restricciones técnicas y requisitos de funcionamiento de la MSN y el

sistema de asistencia sanitaria.

La comunicación fiable y segura entre cualquier par de WMS en una MSN requiere la capacidad de los WMS para establecer directamente una clave por parejas sin depender de un centro de confianza en línea o infraestructura de clave pública según lo descrito anteriormente. El presente sistema puede utilizar dos tipos diferentes de enfoques de distribución de claves para manejar las claves criptográficas en función de los requisitos de funcionamiento de la aplicación de asistencia sanitaria deseada. Por un lado, tenemos las llamadas BSN personales que comprenden siempre el mismo conjunto de WMS, ya que siempre son utilizados por el mismo usuario, por ejemplo, en casa. La distribución de claves para estos BSN personales puede resolverse fácilmente mediante la distribución de claves por pares entre todos los nodos por medio de un canal fuera de banda o en un entorno seguro. Por lo tanto, en una BSN *con n* nodos, cada nodo almacena *n-1* claves.

Por otro lado, en los hospitales, las residencias de ancianos o los centros de fitness, las MSN pueden comprender un gran número de WSN. Un subconjunto de WMS puede recogerse al azar a partir del conjunto de WMS de la MSN para comprender una BSN. En esta situación, los sistemas de distribución de claves basados en sistemas de distribución de claves λ seguras, tales como los polinomios Blundo, ofrecen una solución eficiente y factible para la distribución de claves eficiente debido a que requieren pocos recursos computacionales y permiten una conectividad total entre cualquier par de nodos. En este contexto, cada nodo, z, que pertenece a la misma MSN tiene un único $_z$ *identificador ID* vinculado a un conjunto diferente pero correlacionado de material de creación de claves, $KM_{z,}$ transportado por el nodo. Los diferentes conjuntos de material de creación de claves para diferentes nodos son generados fuera de línea por un centro de confianza a partir de un material original de creación de claves (KM^{origen}). Siempre que un par de nodos tiene que ponerse de acuerdo sobre una clave común, intercambian sus IDs de nodo y usan sus respectivos materiales de creación de claves para ponerse de acuerdo sobre una clave de pares para permitir otros servicios de seguridad. En un enfoque, el$KM^{de\ origen}$ es un polinomio de dos variables único *f (x,y)* de grados λ sobre un campo finito $F_{q,}$ con una q suficientemente grande para acomodar una clave criptográfica. Cada WMS, z, recibe del centro de confianza MSN un conjunto de material de creación de claves obtenido de la $KM^{de\ origen}$, $KM_{z,}$ por ejemplo, compuesto de una parte polinomio, *f (z, y),* generada mediante la evaluación del polinomio de dos variables original *en x = z* . Este conjunto de material de creación de claves, $KM_{z,}$ se realiza durante toda la vida de WMS z, y el identificador, $_z$ *ID* puede ser visto como un número de serie que identifica a cada nodo en la MSN. Este enfoque donde la $KM^{de\ origen}$ es un polinomio de dos variables se puede combinarse con la segmentación tecla o técnicas combinatorias para mejorar el rendimiento y la capacidad de recuperación del sistema en los sistemas de distribución de claves λ seguras. Para simplificar, se considera que cada KM_z llevado por un WMS se compone de una parte polinomio *f (z, y).*

Este enfoque permite un acuerdo de claves distribuidas eficiente, pero no permite la implementación ligera de los servicios de seguridad como el control de acceso en las MSN, un asunto importante de seguridad en aplicaciones médicas. Esto se debe al identificador único, z, vinculado al KM_z llevado por cada nodo z, y que requiere una gran cantidad de memoria para almacenar listas de control de acceso. Por otra parte, el uso de un único dominio seguro SD de λ seguras implica que la captura de λ WMS en un SD MSN permite a un atacante comprometer la seguridad de toda la MSN.

Para superar ambos problemas, es posible tener en cuenta el modelo de implementación de las MSN objetivo para distribuir KM de λ seguras adicional para WMS de una manera inteligente. Para entender esto, observe que un WMS que pertenece a una MSN pueden subdividirse en varias sub-SD estándar según diferentes características, tales como la propiedad, la zona de operaciones o la especialidad médica. Por ejemplo, el WMS de una MSN de hospital se puede clasificar según (i) ubicación (una MSN médica puede comprender varios hospitales, y cada uno de estos hospitales puede ser dividido en diferentes departamentos); (Ii) la especialidad médica como los departamentos ubicados en diferentes hospitales puede compartir la misma especialidad médica; o (iii) la zona operativa como los pacientes que sufren de una enfermedad específica puede ser tratada en diferentes departamentos médicos. El TC del centro de confianza de MSN (ver la fig. 6) puede asignar material de creación de claves λ seguras adicional a WMS con el fin de identificar y autentificar a cuál de los sub-SD y WMS previamente mencionados pertenece de una manera discreta. Cada característica, *j* con $1 \leq j \leq n,$ puede describir un SD plana o una infraestructura jerárquica de SD. Un SD plana comprende un subconjunto de WMS de la MSN que puede comunicarse con la misma probabilidad *p,* por ejemplo, el WMS utilizado en la misma zona de operaciones. Una infraestructura jerárquica de SDs describe las relaciones entre los nodos, por ejemplo, debido a la ubicación WMS. Por ejemplo, la ubicación de un nodo se puede dividir en hospital y/o departamento. En este ejemplo, está claro que todos los WMS en un hospital deben poder comunicarse entre sí, pero también que las comunicaciones entre WMS pertenecientes a un departamento dado son más frecuentes ya que se producen en la misma ubicación. De hecho, la comunicación entre WMS de diferentes departamentos rara vez puede ocurrir, y se producen solo si, por ejemplo, un paciente se traslada a otro departamento. La siguiente fórmula puede utilizarse para asignar los sub-identificadores de $ID_{ij,}$, para la sub-SDS hasta un WMS con identificador ID: $ID_{ji} = h\ (ID|j|i)$.

En esta expresión, *h (•)* es una función de hash criptográfica, *j* identifica una característica WMS como la ubicación o la propiedad, e i se refiere al nivel en la jerarquía de SD, por ejemplo, para la ubicación, el hospital se encuentra en el nivel 1, y el departamento en el nivel 2. Tenga en cuenta que el material de creación de claves vinculadas a cada

una de estos sub-SDs se puede generar a partir de una KM_{ij}^{root} diferente, como, por ejemplo, un *polinomio* $f_{ij}(x, y)$de dos variables diferentes pero que los identificadores utilizados en cada sub-SD están unidos por medio de (1) para evitar que un atacante cree identidades arbitrarias con características arbitrarias. Tenga en cuenta que la convención de nomenclatura anterior podría fácilmente adaptarse o modificarse o simplificarse.

La figura 8 representa la información transportada por un WMS en una MSN particular. El WMS tiene un identificador de MSN único *ID de MSN* vinculado al material de creación de claves *KM MSN.* Esta información permite la plena interoperabilidad entre cualquier par de WMS en el mismo MSN. Tenga en cuenta que ID_{MSN} puede asignarse a diferentes dispositivos o personal médico, de tal manera que depende de su identidad digital. Además, el WMS también lleva el material de creación de claves que se identifica y autentifica a sí mismo según tres funciones diferentes, a saber la ubicación (edificio y planta), la zona de funcionamiento, y la especialidad médica.

Basándose en esta información, dos WMS pertenecientes a la misma MSN pueden establecer un canal de comunicación seguro de una manera eficiente (vea la fig. 9). En un primer paso, un *WMS 1,* por ejemplo, un PDA clínico, envía una solicitud de comunicación para *WMS 2,* por ejemplo, un WMS de ECG conectado a un paciente. *WMS 2* solicita la identificación del PDA como perteneciente al MSN. Adicionalmente, las políticas de control de acceso de ese paciente pueden requerir que el médico tenga una identidad digital específica ID_{MSN} o pertenezca al mismo hospital y los mismos sub-SD de zona de funcionamiento (funciones necesarias). En general, podría ser necesario autorizar cualquier subconjunto de sub-SDS para llevar a cabo una instrucción. Este enfoque permite el control de acceso criptográficamente forzado. En tercer lugar, los dos WMS llevan a cabo un protocolo de intercambio acuerdo de claves. Para este fin, cada WMS calcula una clave parcial, $K_{ji,}$ desde el material de creación de claves vinculado a cada (sub-) SD requerida, *ji, ji* KM, para ser autentificado. K_{ji} se calcula mediante la evaluación de $KM_{ji,}$ es decir, la cuota de polinomio $_{ij}(h(ID|j|i),$ en el identificador de la otra parte para que (sub-)SD. Ambos nodos pueden generar una clave principal K mediante hashing de todas las claves parciales en el mismo orden. La clave principal K será común a ambos WMS, si cada una de las claves parciales es idéntica. Esta clave se utiliza posteriormente para autentificar los dos WMS por medio de un protocolo de autentificación de desafío - respuesta. La autentificación exitosa también implica que el médico cumple con las políticas de control de acceso para el paciente. Tenga en cuenta que el enfoque de distribución de claves de base de este ejemplo se puede extender fácilmente a un establecimiento de claves λ seguras general multidimensional mλKE con un número arbitrario de *sub-SDs ji* donde la principal *ID* codifica la identidad digital de un dispositivo y los sub-SDs representan las funciones del dispositivo. Además, la ID puede utilizarse para codificar la identidad digital de la entidad u otra información, como las funciones de control de acceso mediante el cálculo de ID=h (identidad digital) como se describe en el estado de la técnica

Además de garantizar una comunicación segura entre WMS, el sistema de seguridad divulgado debe habilitar la seguridad integral entre WMS en BSN y los servicios de asistencia sanitaria finales. Este sistema utiliza una solución basada en la infraestructura de clave pública PKI para esto ya que permite a los usuarios moverse a través de MSN de una manera segura, y por lo tanto, garantiza la interoperabilidad. Observar que otros enfoques, por ejemplo, sobre la base de un tercero de confianza, por ejemplo, Kerberos, podrían también aplicarse para lograr el mismo objetivo. En un enfoque basado en clave pública, cada usuario en el sistema requiere un par de claves públicas / privadas emitidas por una autoridad de certificación de asistencia sanitaria HSP (centralizado o distribuido) (vea la fig. 6) y vinculadas a la identidad del usuario. Este par de claves solo se utiliza durante el procedimiento de configuración inicial que tiene lugar cuando un usuario llega a una MSN, como se describe a continuación, de modo que se reduzcan al mínimo las necesidades de recursos (véase la figura 6 y la fig. 12). Sin embargo, lo que garantiza que BSN de un usuario siempre contenga este par de claves es una tarea difícil ya que la pertenencia a una BSN es impredecible, como se ha descrito anteriormente. La solución a estos problemas se presenta a continuación.

Asociación de BSN segura

El sistema divulgado se basa en y extiende el protocolo de asociación BSN descrito anteriormente para permitir la asociación BSN segura, tal como se representa en la figura 10. Un WMS especial, llamado administrador de seguridad personal PSM o administrador seguridad personal extendido PSMx, (vea las figuras. 7, 10 y 11) juega el papel de un identificador personal, ya que se utiliza para transmitir el identificador del paciente a otros WMS conectados al paciente, y por lo tanto, vinculando los WMS a la identidad del usuario. La comunicación entre PSM y WMS puede basarse en la comunicación acoplada al cuerpo, y por lo tanto, se puede restringir a los dispositivos acoplados directamente al cuerpo de un paciente.

En primer lugar, antes de transferir la ID del paciente a un WMS o aceptar un WMS en de la BSN (Fig. 10, paso 1), el PSM autentifica y autoriza los WMS según los procedimientos de λ seguras descritos anteriormente. Para este fin, el PSM y el WMS pueden utilizar el material de creación de claves λ seguras que ambos nodos llevan para generar una clave principal $K_{PSM-WMS.}$. Sobre la base de esta clave, ambos nodos pueden autentificar y autorizar de manera eficiente entre sí y transmitir más información, por ejemplo, ID de usuario, de una manera segura. Además, el PSM puede desempeñar el papel de centro de confianza de la BSN que genera y distribuye una clave BSN, $K_{BSN,}$ a todos

los miembros de BSN. K_{BSN} es la clave de red de dominio de seguridad de la BSN y se puede utilizar para permitir la emisión dentro de la BSN y para convertir de la BSN en un SD independiente, que es controlado por la BSN del usuario, dentro del SD de MSN.

La clave de red K_{BSN} en combinación con BCC también puede permitir la implementación sin esfuerzo de un procedimiento de revocación de WMS. Esto es necesario cuando se captura un nodo o se deja una BSN de un paciente. Para este fin, el PSM envía solicitudes periódicas a cada miembro de la BSN por la BCC. Si el PSM no recibe una respuesta de ninguna de ellas, el PSM actualiza tanto el identificador de usuario como la clave de BSN, K_{BSN} con el fin de proteger la privacidad del usuario. El nuevo identificador y la clave de BSN se envían a los miembros de BSN de una manera segura mediante el uso de las comunicaciones acopladas al cuerpo y la clave de pares correspondiente. Por último, el PSM podría transmitir una secuencia aleatoria de todos los WMS en la BSN. El WMS puede sincrónicamente parpadear después de esta secuencia aleatoria con el fin de permitir a los médicos comprobar la asociación de BSN correcta de todos los WMS de una manera simple.

Identificación de usuario inequívoca y única

Las BSN deben verse como SDS completamente independientes en una MSN, donde las interacciones de seguridad con WMS y usuarios de otros MSN se manejan por medio del PSM. Además, el PSM debe proveer información de asistencia sanitaria electrónica (EHI) de usuarios y usuarios globales, así como otros servicios de seguridad, por ejemplo, auditoría, gestión de las políticas de control de acceso, o seguridad integral.

Con el fin de enlazar los signos vitales del usuario con el identificador único del usuario, que es independiente de la MSN en el que se encuentra el usuario en un momento específico, el sistema de seguridad divulgado puede utilizar la HCC de tarjeta de asistencia sanitaria en combinación con el PSM para formar un administrador de seguridad personal extendido PSMx. El PSMx conecta los diferentes dominios de seguridad de MSN con el sistema de asistencia sanitaria omnipresente, es decir, el PSMx organiza las relaciones de seguridad entre los WMS que componen BSN del usuario en una MSN específica y servicios de asistencia sanitaria finales para lograr la identificación del usuario inequívoca y única en MSN omnipresentes.

El PSMx puede consistir en varios bloques funcionales independientes (ver la fig. 11). En primer lugar, puede almacenar la KM de material de creación de claves λ seguras para habilitar la comunicación segura con WMS de la MSN, como se ha descrito anteriormente. El PSMx puede estar preconfigurado con KM de λ seguras o activar su configuración dinámica en un entorno seguro durante la fase de instalación. El PSMx también puede almacenar un certificado expedido por el centro de confianza MSN local. El propósito de este certificado es permitir que el usuario y la HCC de usuario autentifiquen la autenticidad del PSM cuando se une a una MSN. En segundo lugar, el PSMx puede implementar un lector de tarjetas inteligentes (ranura HCC) de manera que la tarjeta de asistencia sanitaria del usuario puede ser conectarse. El sistema divulgado utiliza la HCC con fines de identificación para su uso en aplicaciones médicas. Los sistemas de seguridad de la asistencia sanitaria omnipresente deben ser totalmente compatibles con él. En un modo de realización, la información médica más relevante de usuario se almacenará en la HCC, por ejemplo, nombre, identificador, y registro médico o políticas de AC control de acceso de usuario para diferentes MSN. Además, la HCC también puede almacenar claves públicas / privadas emitidas por la CA de asistencia sanitaria global Por último, el PSMx puede implementar un protocolo de seguridad para habilitar la autentificación mutua de PSMx y HCC, seguridad integral, auditoría y gestión de las políticas de privacidad de control de acceso de contexto.

La combinación de la HCC con el PSM para crear el PSMx garantiza la interoperabilidad entre diferentes MSN y sistemas finales. Por un lado, la información de seguridad almacenada en la HCC identifica y autentifica al usuario, actuando como puente entre BSN del usuario y los servicios de asistencia sanitaria centralizados donde se encuentra el usuario. Esto incluye el uso de un ID de usuario regulado, o un seudónimo temporal obtenido a partir del identificador según un procedimiento regulado, que se utiliza en todo el sistema para lograr la identificación de usuario inequívoca a través de una variedad de escenarios de aplicación.

La clave pública del usuario se utiliza para autentificar el ID de usuario y configurar una comunicación segura entre de la BSN y los servicios de asistencia sanitaria finales. Por otro lado, el PSMx, en el que se inserta la HCC, almacena la KM de λ seguras que permite comunicaciones seguras con WMS en el mismo MSN. Por lo tanto, esta construcción permite la creación de un enlace seguro integral entre los WMS que comprenden una BSN de un usuario y los servicios de asistencia sanitaria omnipresentes centralizados, incluso si los pacientes se mueven de una MSN a otra. Además, un PSMx puede conmutarse para dar cabida a un nuevo paciente mediante el intercambio de HCC (vea las figs. 6, 7 y 11). Los modos de realización del PSMx pueden variar desde un teléfono móvil con una ranura para tarjeta inteligente adicional para la HCC a una pulsera llevada por los pacientes en un hospital.

Además, el PSMx también puede gestionar dinámicamente las políticas de CA de control de acceso (vea la fig. 10) para un paciente. Estas políticas de control de acceso pueden combinarse con técnicas de control de acceso λ seguras como se explicó anteriormente. En este contexto, el PSMx puede manejar las políticas de CA locales en la MSN actual con las políticas de CA globales controladas por los servicios de asistencia sanitaria finales. Las técnicas

sensibles al contexto se pueden utilizar para mejorar las políticas de control de acceso, por ejemplo, para permitir el acceso a la BSN de un paciente a cualquier médico cuando se detecta una situación de emergencia.

Por último, una característica importante de nuestro sistema de seguridad es que de la BSN forma un dominio seguro SD autónomo donde el PSMx es el centro de la confianza del usuario. Por lo tanto, todas las acciones llevadas a cabo en de la BSN se pueden grabar en HCC del usuario incluso si se pierde la conectividad con el centro de confianza para MSN. Esto garantiza la auditoría de acciones médicas ya que la HCC del usuario puede mantener un registro de todos los dispositivos y los usuarios que lo han intentado tener, o tenido acceso a la BSN del usuario. Por otra parte, las propiedades técnicas de las tarjetas inteligentes evitan el acceso no autorizado a dicha información.

Evaluación del sistema

La evaluación de la arquitectura de seguridad para MSN puede llevarse a cabo a partir de tres puntos de vista ortogonales, a saber, la viabilidad práctica en entornos médicos profesionales, el rendimiento del sistema, y el análisis de seguridad.

Viabilidad práctica: Configuración y despliegue

Un sistema de seguridad para MSN debe ser simple de configurar y desplegar con el fin de minimizar los costos. Además, el personal y los usuarios médicos sin antecedentes técnicos deben ser capaces de manejar de forma intuitiva los aparatos que se les da.

Con el fin de mostrar ambas propiedades, ahora vamos a centrar nuestra atención en la configuración del sistema cuando un usuario de edad avanzada, Robert, va al hospital para un procedimiento médico profesional (ver fig. 6). Cuando Robert llega al mostrador de admisión del hospital, utiliza su HCC para la identificación y el pago. Posteriormente, la HCC se inserta en un PSM para crear un PSMx y se lleva a cabo un protocolo de intercambio de autentificación mutua. El PSMx se configura con la correspondiente KM λ seguras para permitir comunicaciones seguras con WMS, así como con la política de control de acceso local para ese paciente. Esta directiva local se almacena en la HCC del paciente, y en el registro de asistencia sanitaria final del paciente.

Después de la admisión, el paciente recibe un conjunto de WMS, en el diagnóstico, para la monitorización de sus signos vitales. Cada uno de los WMS se comunica con el PSMx del paciente llevando a cabo un protocolo de intercambio de acuerdo de claves, autentificación y autentificación a través de BCC de comunicaciones acopladas al cuerpo. Cada uno de los WMS que termina con éxito este paso se convierte en un miembro de la BSN del paciente, y recibe la clave de red BSN y el identificador del paciente. Las identidades de todos y cada uno de los WMS se almacenan en la HCC del paciente, incluyendo las identidades digitales de PDA para médicos usadas para controlar o tratar a los pacientes. La MSN del hospital ($MSN_{HOSP)}$ puede incluir un número de BSN ($BSN_{x\ Hosp)}$,

El sistema permite iniciar automáticamente una BSN de una manera segura; por ejemplo, cuando un médico quiere monitorizar los signos vitales de un paciente, el médico toca brevemente el paciente para establecer un canal de BCC entre el PSMx y PDA. El PDA de los médicos se une automáticamente a la BSN de Robert de una manera segura, a través de acuerdo de claves, la autentificación y autorización según las políticas de control de acceso, y recibe el seudónimo del paciente y $K_{BSN.}$ El resto de WMS de la BSN del paciente recibe la dirección del PDA desde el PSMx para que puedan comenzar a transmitir signos vitales del paciente al PDA de una manera segura.

El sistema también puede implementar políticas de privacidad y control de acceso sensibles al contexto dinámicas que permiten la adaptación dinámica de las reglas de control de acceso. Por ejemplo, si un paciente sufre un ataque al corazón, el WMS puede enviar una alarma al PSMx, de modo que el PSMx puede autorizar a un médico para cuidar del paciente. Tenga en cuenta que la mλKE todavía garantiza una comunicación segura en estas situaciones, ya que todos los WMS en la MSN comparten KM correlacionada del SD de MSN principal, y por lo tanto cualquier par de WMS en la MSN puede ponerse de acuerdo sobre una clave común de pares.

Rendimiento de sistema

El rendimiento del sistema de seguridad divulgado se analizó en los dispositivos con recursos limitados, es decir, WMS, PSM y la HCC, ya que representan los cuellos de botella del sistema. La plataforma WMS puede incluir las características de MicaZ como se describe anteriormente. Se supone que un total de 2 Kbytes están reservados para KM de λ seguras y se utilizan claves de 64 bits. Por último, se supone que las capacidades y el rendimiento criptográficos de la HCC son similares a, por ejemplo, la uPD789828 de NEC. La tabla 1 (fig. 13) compara el rendimiento de algunas primitivas de seguridad en MicaZ y uPD789828.

Ahora podemos describir la eficiencia de la mλKE, según el modo de realización de diversos protocolos de establecimiento de claves para redes de sensores inalámbricos basados en polinomios Blundo. La evaluación de un polinomio de orden λ y una clave de 64 bits requiere 500•λ ciclos de CPU que a 8 MHz tarda 0,0625 • λ mseg. El

enfoque clave de distribución, como se describe más arriba, requiere la evaluación de varios polinomios con un tamaño máximo de hasta 2 Kbytes, es decir, un total de 256 coeficientes distribuido entre los diferentes polinomios. Por lo tanto, cuando se utiliza 256 como λ, el tiempo de evaluación de polinomio se puede aproximar a 16 mseg. El cómputo de los identificadores para cada uno de los sub-SD de una MSN, la clave principal, la generación de una clave de sesión o el protocolo de enlace de autentificación requiere el uso de una función hash. Sin embargo, una función hash puede implementarse de manera eficiente mediante la implementación de hardware de AES disponible en el MicaZ. Por ejemplo, la aplicación de la función de hash Matyas-Meyer-Oseas, también usado en ZigBee, un cálculo de hash de 16 bytes tarda menos de 12 microsegundos. Por lo tanto, el tiempo total de cálculo en este ejemplo específico se puede aproximar a 16 mseg. Este valor indica que este enfoque es mucho más rápido que las soluciones de clave pública. Por otra parte, tiene dos ventajas adicionales: En primer lugar, un par de WMS solo necesita intercambiar sus identificadores de MSN (2 bytes) y los identificadores de sub-SDS hasta ser autentificados. Esto reduce la sobrecarga de comunicación en comparación con el intercambio de claves públicas largas, lo cual ayuda a prolongar la vida útil de la batería del WMS. En segundo lugar, este enfoque permite a la aplicación de las políticas de control de acceso sin almacenar las listas de control de acceso largas o que requieren el uso de firmas digitales que requieren una clave pública cara. En consecuencia, y suponiendo que una BSN comprenda alrededor de 10 WMS, el sistema descrito permite la asociación BSN segura en un tiempo de alrededor de 160 mseg. incluyendo el acuerdo de clave y de control de acceso inherente, que es mucho más rápido que un solo cálculo de clave pública (véase la tabla 1 (fig. 13) para la comparación) y cumple con los requisitos de latencia de transmisión de ECG y configuración de BSN.

Utilizando primitivas criptográficas ligeras para las operaciones frecuentes, el sistema descrito libera WMS de las operaciones computacionalmente intensivas y reduce el uso de la criptografía de clave pública solo a los protocolos de intercambio de seguridad entre la HCC, PSM y el centro de confianza de asistencia sanitaria central para configurar el PSMx. Estos protocolos de intercambio ocurren solo esporádicamente en entornos seguros durante la configuración de PSMx inicial. Por lo tanto, el sistema no es propenso a los ataques de DoS.

Análisis de seguridad

El establecimiento de claves λ seguras multidimensionales mλKE permite un rápido acuerdo de claves mediante el uso de enfoques descentralizados de distribución de claves. Sin embargo, un sistema de distribución de claves λ seguras adolece del inconveniente de que la combinación de los conjuntos de material de creación de claves independientes λ permite a los atacantes romper la seguridad del sistema, es decir, recuperar la $KM^{de\ origen}$ original. En esta sección, se analiza cómo el enfoque divulgado de distribución de claves seguras λ multidimensionales no solo permite distribuir el control de acceso, sino que también optimiza la capacidad de recuperación del sistema, por lo que es posible alcanzar un nivel de seguridad alto. A partir de aquí, el término capacidad de recuperación, α, representa la fracción de comunicaciones que se ve comprometida después de capturar k nodos en un SD (dominio seguro) en base a un sistema de distribución de claves λ seguras. Observe que $0 \leq \alpha \leq 1$, y que $\alpha = 1$ cuando $k = \lambda$ si un solo polinomio se utiliza en un SD. Denominamos capacidad de recuperación relativa, α_r, a la relación entre el número de nodos comprometidos para hacer α=1, es decir, λ, y el número total de WMSs, n_{ji}, en SD_{ij} Obsérvese que un sistema de λ seguras con α_r mayor que 1 es perfectamente seguro y que dados dos SD de λ seguras con igual capacidad de recuperación, el que tiene α_r más cerca de 1 puede ser considerado más seguro ya que un intruso debe capturar la misma cantidad de los nodos de un conjunto más pequeña de WMS. Por lo tanto la resistencia es una medida de la resistencia de los sistemas para, y para protegerse de, compromiso de nodo.

Para descifrar el mλke, un atacante debe comprometer cada uno de los (sub-)SD. Del mismo modo, para romper la seguridad de las comunicaciones con un WMS, un atacante debe romper todos los SDs de λ seguras desde los cuales el WMS tiene KM λ seguras. De este modo, para la KM representada en la fig. 8, un atacante debe romper un total de 5 SD estándar para comprometer las comunicaciones. A pesar del hecho de que un solo SD de λ seguras, por ejemplo, el SD de MSN, es relativamente fácil de romper debido a que todos los dispositivos llevan un conjunto de KM del mismo y un atacante puede adquirir con un esfuerzo relativamente pequeño una pequeña fracción de los mismos, romper el resto de sub- SD es mucho más difícil. Esto se debe a que la capacidad de recuperación relativa de estos SD es más alta y solo algunos nodos en la KM correlacionado de la propia MSN. Por lo tanto, si un atacante intenta eliminar muchos de los WMS en el mismo (sub-)SD, se puede detectar fácilmente. Además, la cantidad de información de λ seguras que un atacante tiene que obtener con el fin de romper todos los incrementos de comunicación cuando se utilizan múltiples SDs de λ seguras e incluso si uno de ellos se ve comprometida el resto permanecen seguros.

En general, la resistencia y la capacidad de recuperación relativa del mλKE donde una *clave K* principal se calcula como el hash de varias claves parciales, $K_{ji,}$ generada a partir de varias desviaciones estándar λ seguras, $_{ji}$ $SD,$ viene dada por las fórmulas (2) y (3), respectivamente:

Formula (2) $$\alpha^{m\lambda KE} = Max\left\{\forall_{ji}\left\{n_{ji}`\alpha_{ji}\right\}\right\}$$

Formula (3) $$\alpha_r^{m\lambda KE} = Max\left\{\alpha_r^1,..,\alpha_r^h,...,\alpha_r^K\right\}$$

Ejemplo - suponemos una MSN de hospital que comprende un total de 1.000 WMS (~ 100 BSN de pacientes); dos edificios, cada edificio dividido en 5 plantas; y un total de 10 zonas de operaciones y 8 especialidades médicas diferentes. También suponemos el uso de 2 Kbytes de memoria para asignar KM de λ seguras. A cada sub-SD se le asigna una cantidad de memoria como se describe en la tabla 2 (fig. 14) y suponiendo una distribución uniforme de WMS para los SD, se puede calcular la capacidad de recuperación y capacidad de recuperación relativa para cada sub-SD. A partir de estos valores, se puede concluir que un atacante debe comprometer 385 nodos, es decir, el 38,5% del conjunto de WSN, para romper este sistema específico.

Aunque la invención se ha ilustrado y descrito en detalle en los dibujos y la descripción anterior, dicha ilustración y descripción han de considerarse ilustrativas o como ejemplo y no restrictivas; la invención no se limita a los modos de realización divulgados. Los expertos en la técnica pueden entender y efectuar otras variantes de los modos de realización divulgados al poner en práctica la invención reivindicada, a partir de un estudio de los dibujos, de la divulgación y de las reivindicaciones adjuntas.

En las reivindicaciones, las palabras "que comprende" no excluyen otros elementos o pasos, y el artículo indefinido "un" o "una" no excluye una pluralidad. Un único elemento, u otra unidad, puede cumplir las funciones de varios elementos citados en las reivindicaciones. El mero hecho de que ciertas medidas se citen en reivindicaciones dependientes diferentes entre sí no indica que no pueda utilizarse una combinación de estas medidas de manera más ventajosa.

Cualquier signo de referencia en las reivindicaciones no se interpretará como una limitación del alcance.

REIVINDICACIONES

1. Un sistema integral de asistencia sanitaria al paciente, que comprende:

- uno o más sensores médicos inalámbricos adaptados para acoplarse al cuerpo de un paciente y en comunicación entre sí formando una red de sensores corporales dentro de una red de sensores médicos inalámbrica que incluye una o más redes de sensores corporales;

- medios de creación de claves λ seguras incorporados en cada uno de dichos sensores médicos inalámbricos para habilitar las comunicaciones seguras entre dichos sensores médicos inalámbricos, y

- un administrador de seguridad personal dentro de la red de sensores corporales y en comunicación con dicho uno o más sensores médicos inalámbricos dentro de dicha red de sensores corporales, con dicho administrador de seguridad personal proporcionando comunicaciones seguras con los servicios finales y proporcionando relaciones de seguridad dentro de dicha red de sensores corporales mediante medios de creación de claves λ seguras

En el que dichos medios de creación de claves λ seguras son tales que una coalición de no más de λ sensores médicos inalámbricos comprometidos esconde una clave de pares entre dos sensores médicos no comprometidos inalámbricos y proporciona protección contra compromiso de nodo hasta que λ+1 sensores médicos inalámbricos se han comprometido,

- una tarjeta de asistencia sanitaria conectada al administrador de seguridad personal para formar un administrador de seguridad personal extendido (PSMx), en el que la tarjeta de asistencia sanitaria (HCC) incluye información de identificación e información de seguridad para la comunicación segura con los servicios de asistencia sanitaria finales, en el que el administrador de seguridad personal incluye una certificado expedido por un centro de confianza a nivel local, y en el que el sistema está adaptado para ejecutar un protocolo de seguridad para la auditoría y/o control de acceso y/o protección de la privacidad, y/o una autentificación mutua del administrador de seguridad personal con la tarjeta de asistencia sanitaria.

2. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 1, en el que dichos sensores médicos inalámbricos y dicho administrador de seguridad personal están adaptados para comunicarse por medio de comunicaciones acopladas al cuerpo.

3. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 1 o 2, en el que la información de la red de sensores corporales está vinculada a la identidad del paciente,

en el que dicha tarjeta de asistencia sanitaria del paciente (HCC) y dicho administrador de seguridad personal (PSM) forman un administrador de seguridad personal extendido (PSMx) para conectar una serie de dominios de seguridad de redes de sensores médicos inalámbricos a un sistema de asistencia sanitaria omnipresente, estando dicho administrador de seguridad personal extendido adaptado para:

- almacenar dicho certificado expedido por dicho centro de confianza a nivel local,

- almacenar dichos medios de creación de claves de λ seguras para el establecimiento de una comunicación de seguridad integral emitida por los servicios de asistencia sanitaria centralizados y

- la implementación de dicho protocolo de seguridad para habilitar la autentificación mutua de dicho administrador de seguridad personal extendido y dicha tarjeta de asistencia sanitaria, seguridad integral y/o auditoría, y/o la gestión de las políticas de privacidad y control de acceso de contexto.

4. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 3, en el que dicho administrador de seguridad personal extendido está adaptado para autentificar el administrador de seguridad personal del paciente y la tarjeta de asistencia sanitaria del paciente cuando el paciente se une a la red de sensores médicos.

5. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 3, en el que dicho administrador de seguridad personal comprende un lector de tarjetas inteligentes adaptado para recibir dicha tarjeta de asistencia sanitaria, y en el que dicha tarjeta de asistencia sanitaria incluye información individual de identificación y/o información médica y/o material de seguridad y/o políticas de seguridad.

6. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 5, en el que dicho administrador de seguridad personal incluye un nombre de usuario, identificador, materiales de seguridad, registros médicos o políticas de control de acceso para diferentes redes de sensores médicos.

7. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 5, en el que dicho administrador de seguridad personal extendido incluye la identificación de un usuario global, red de área de paciente, e información de asistencia sanitaria electrónica (EHI) individual, con la información de asistencia sanitaria electrónica (EHI) procedente de dicha red de área de paciente.

8. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 3, en el que se proporciona la información de seguridad almacenada en la tarjeta de asistencia sanitaria para identificar y autentificar al usuario y que actúa como un puente entre la red de sensores corporales del paciente y los servicios de asistencia sanitaria centralizados o finales.

9. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 3, en el que dicho administrador de seguridad personal extendido es un teléfono móvil con una ranura para tarjeta inteligente adicional para la tarjeta de asistencia sanitaria.

10. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 4, que comprende además un dominio seguro autónomo formado por el sensor médico inalámbrico asociado con una red de sensores corporales, en el que dicho administrador de seguridad personal extendido es el centro de confianza de la red de sensores corporales y está adaptado para el control de la asociación o revocación segura de los miembros de la red de sensores corporales.

11. El sistema seguro integral de asistencia sanitaria al paciente de la reivindicación 10, en el que dicho administrador de seguridad personal extendido y dichos sensores médicos inalámbricos están adaptados para almacenar de forma segura información intercambiada y las acciones llevadas a cabo en la red de sensores corporales en la tarjeta de asistencia sanitaria del paciente, incluso si se pierde la conectividad del centro de confianza de la red de sensores médicos.

12. Un procedimiento para la comunicación con el paciente de la asistencia sanitaria integral segura en un sistema seguro integral de asistencia sanitaria al paciente, según la reivindicación 1, que comprende los pasos de:

- almacenar un certificado emitido por un centro de confianza de red de sensores médicos local en el administrador de la seguridad personal;

- formar un administrador de seguridad personal extendido mediante el uso de una tarjeta de asistencia sanitaria en combinación con un administrador de seguridad personal

- proporcionar información de identificación y e información de seguridad mediante el uso de la tarjeta de asistencia sanitaria para el establecimiento de una comunicación de seguridad integral entre sensores médicos inalámbricos y servicios de asistencia sanitaria centralizados; e

- implementar de un protocolo de seguridad para habilitar la autentificación mutua del administrador de seguridad personal y una tarjeta de asistencia sanitaria, seguridad integral, auditoría, y/o la gestión de las políticas de privacidad de control de acceso y contexto.

13. Un administrador de seguridad personal para un sistema seguro integral de asistencia sanitaria al paciente, en el que el administrador de seguridad personal se encuentra dentro de una red de sensores corporales y en comunicación con uno o más sensores médicos inalámbricos dentro de dicha red de sensores corporales, con dicho administrador de seguridad personal que proporciona comunicaciones seguras con servicios finales y proporciona relaciones de seguridad dentro de dicha red de sensores corporales por medio de dichos medios de creación de claves λ seguras, en el que dichos uno o más sensores médicos inalámbricos están adaptados para acoplarse al cuerpo de un paciente y en comunicación entre sí para formar dicha red de sensores dentro de una red de sensores médicos inalámbricos que incluye una o más redes de sensores corporales;
Medios de creación de claves λ seguras incorporadas en cada uno de dichos sensores médicos inalámbricos para habilitar las comunicaciones seguras entre dichos sensores médicos inalámbricos, y
En el que dichos medios de creación de claves λ seguras son tales que una coalición de no más de λ sensores médicos inalámbricos comprometidos esconde una clave de pares entre cualquier par de sensores médicos inalámbricos no comprometidos y proporciona protección contra compromiso de nodos hasta que λ+1 sensores médicos inalámbricos han sido comprometidos

- una tarjeta de asistencia sanitaria conectada al administrador de seguridad personal para formar un administrador de seguridad personal extendido (PSMx), en el que la tarjeta de asistencia sanitaria (HCC) incluye información de identificación e información de seguridad para la comunicación segura con los servicios de asistencia sanitaria finales, en el que el administrador de seguridad personal incluye una certificado expedido por un centro de confianza a nivel local, y en el que el sistema está adaptado para ejecutar un protocolo de seguridad para la auditoría y/o control de acceso y/o protección de la privacidad, y/o una autentificación mutua del administrador de seguridad personal con la tarjeta de asistencia sanitaria.

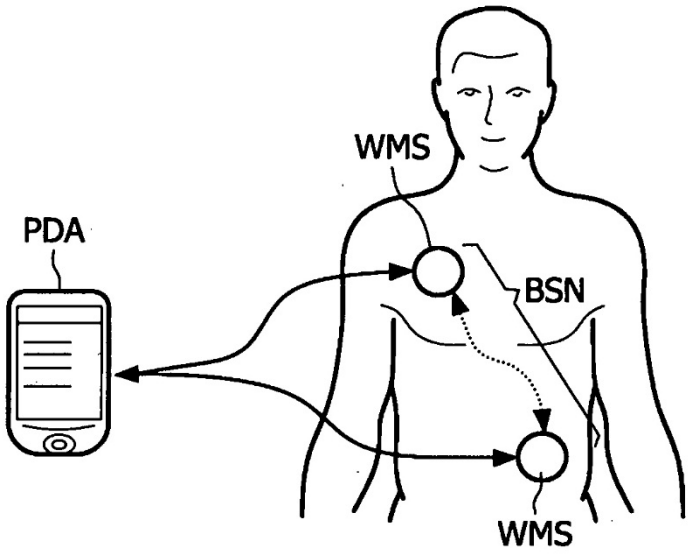

FIG. 1

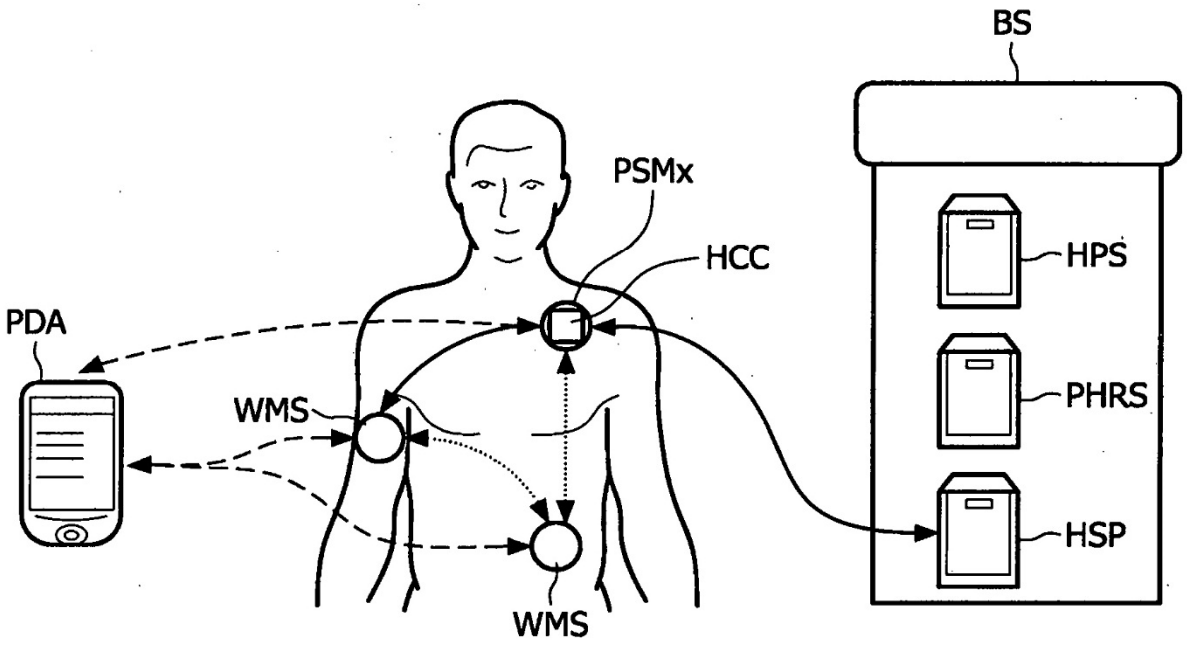

FIG. 2

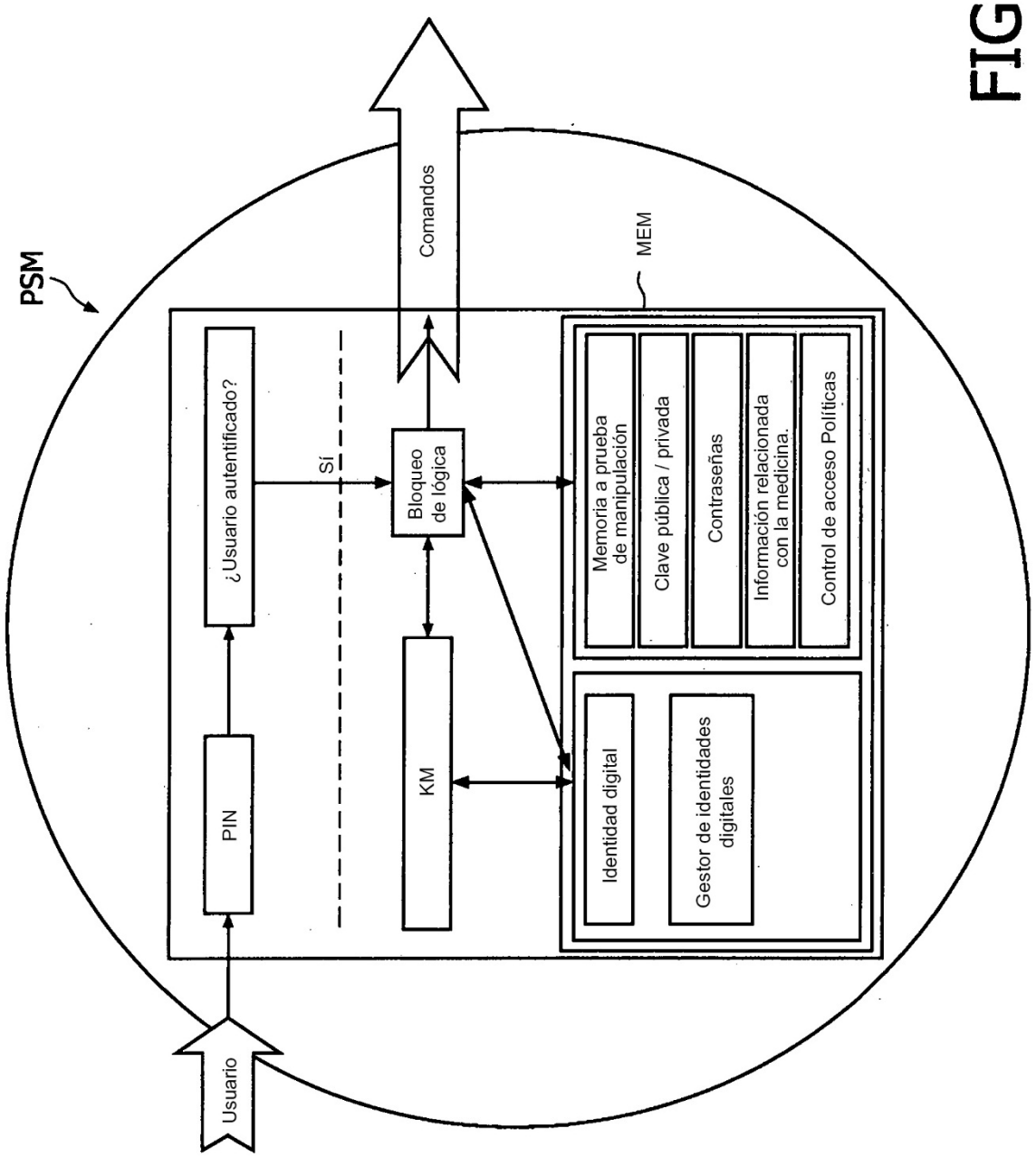
PSM
Comandos
MEM
¿Usuario autentificado?
Sí
Bloqueo de lógica
PIN
KM
Memoria a prueba de manipulación
Clave pública / privada
Contraseñas
Información relacionada con la medicina.
Control de acceso Políticas
Identidad digital
Gestor de identidades digitales
Usuario

FIG. 3

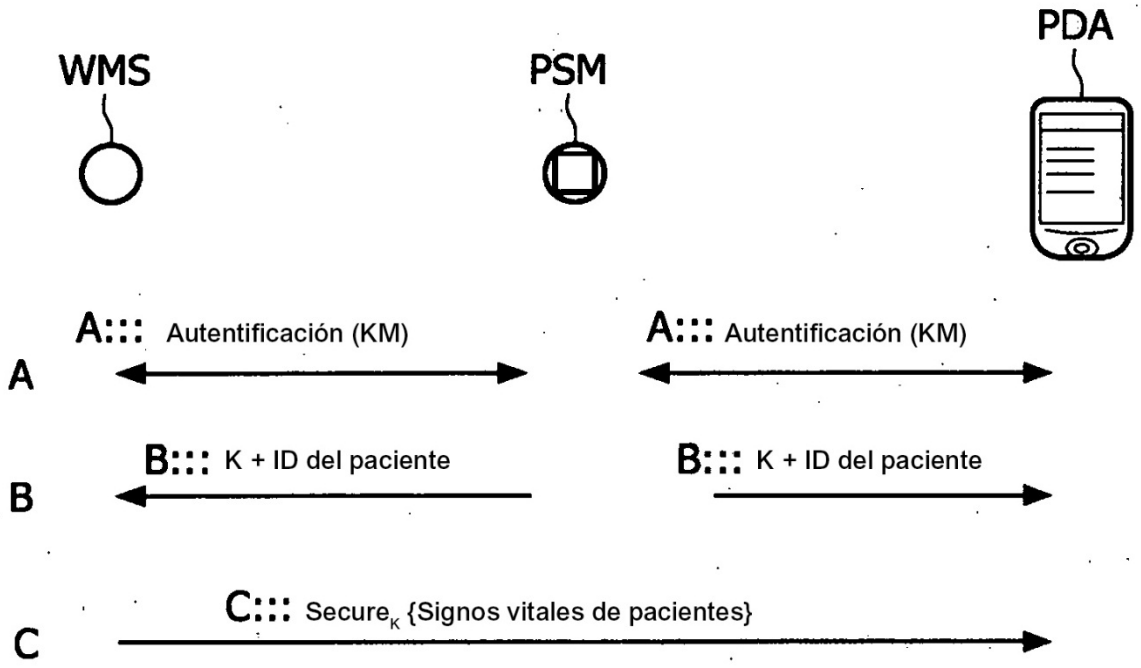
WMS
PSM
PDA
A
A::: Autentificación (KM)
A::: Autentificación (KM)
B
B::: K + ID del paciente
B::: K + ID del paciente
C
C::: Secure$_K$ {Signos vitales de pacientes}

FIG. 4

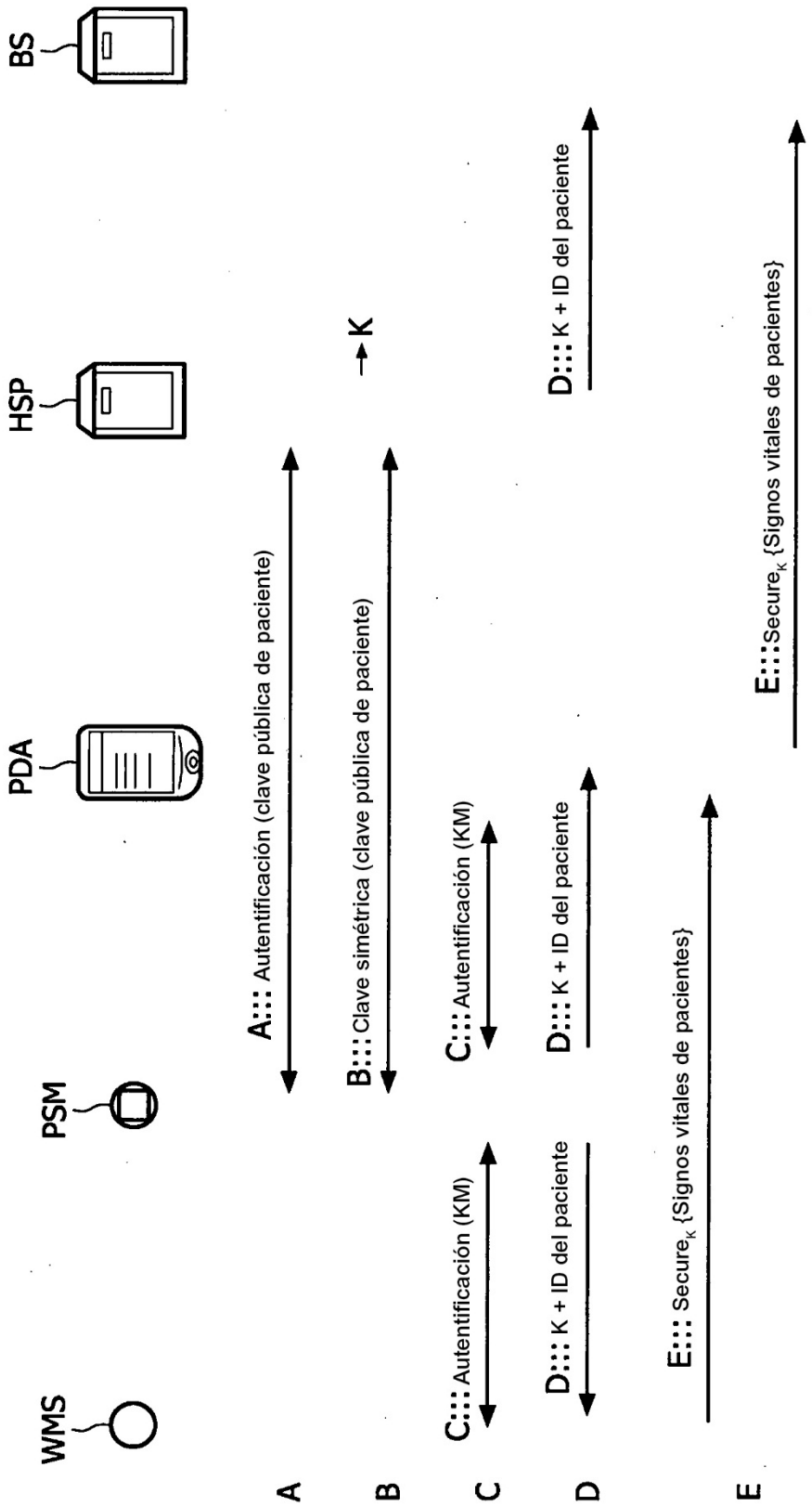
WMS
PSM
PDA
HSP
BS
A
B
C
D
E
A::: Autentificación (clave pública de paciente)
B::: Clave simétrica (clave pública de paciente)
→K
C::: Autentificación (KM)
D::: K + ID del paciente
C::: Autentificación (KM)
D::: K + ID del paciente
D::: K + ID del paciente
E::: Secure$_K$ {Signos vitales de pacientes}
E:::Secure$_K$ {Signos vitales de pacientes}

FIG. 5

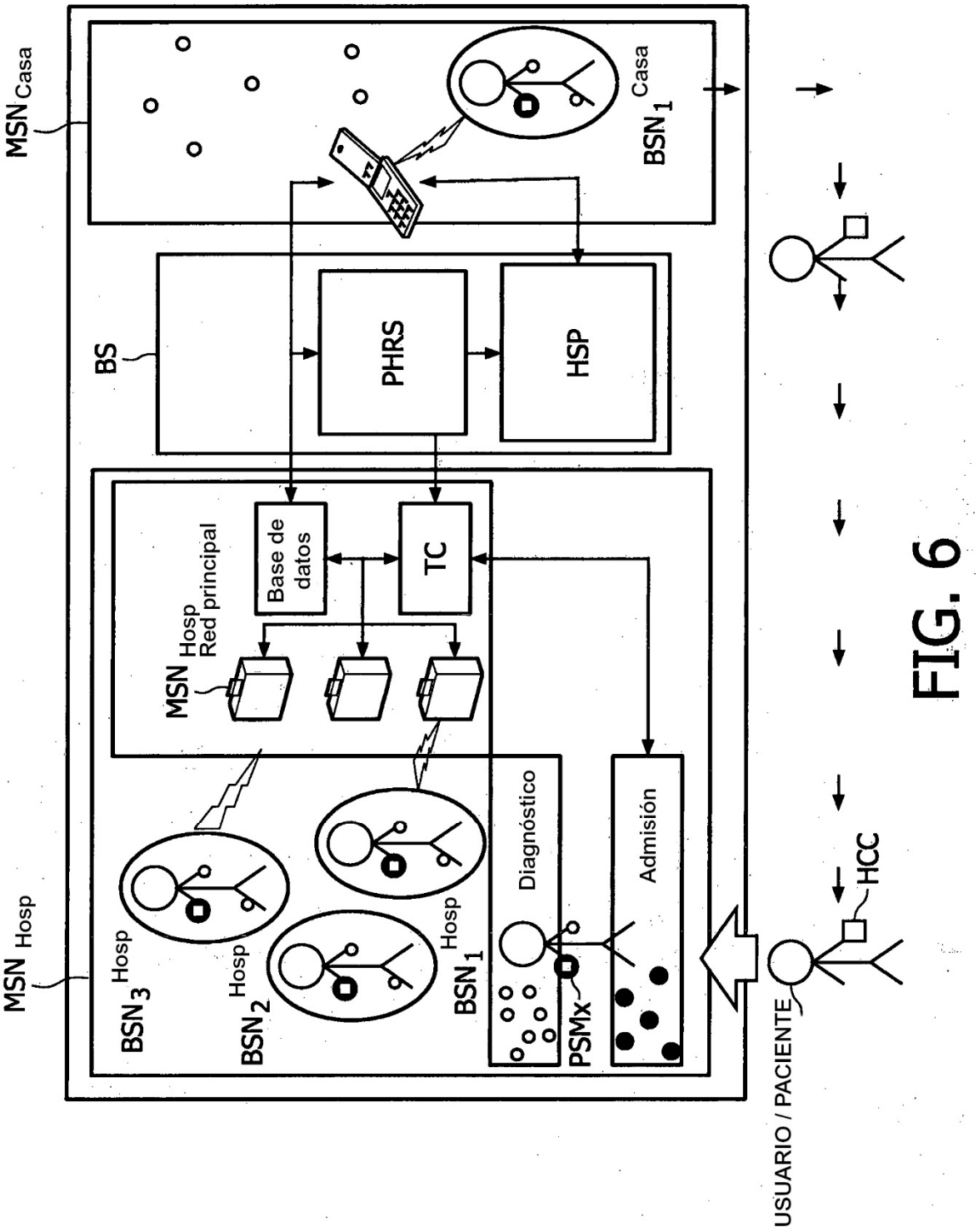
MSN Casa
BSN 1 Casa
BS
PHRS
HSP
MSN Hosp Red principal
Base de datos
TC
MSN Hosp
BSN 3 Hosp
BSN 2 Hosp
BSN 1 Hosp
Diagnóstico
Admisión
PSMx
HCC
USUARIO / PACIENTE

FIG. 6

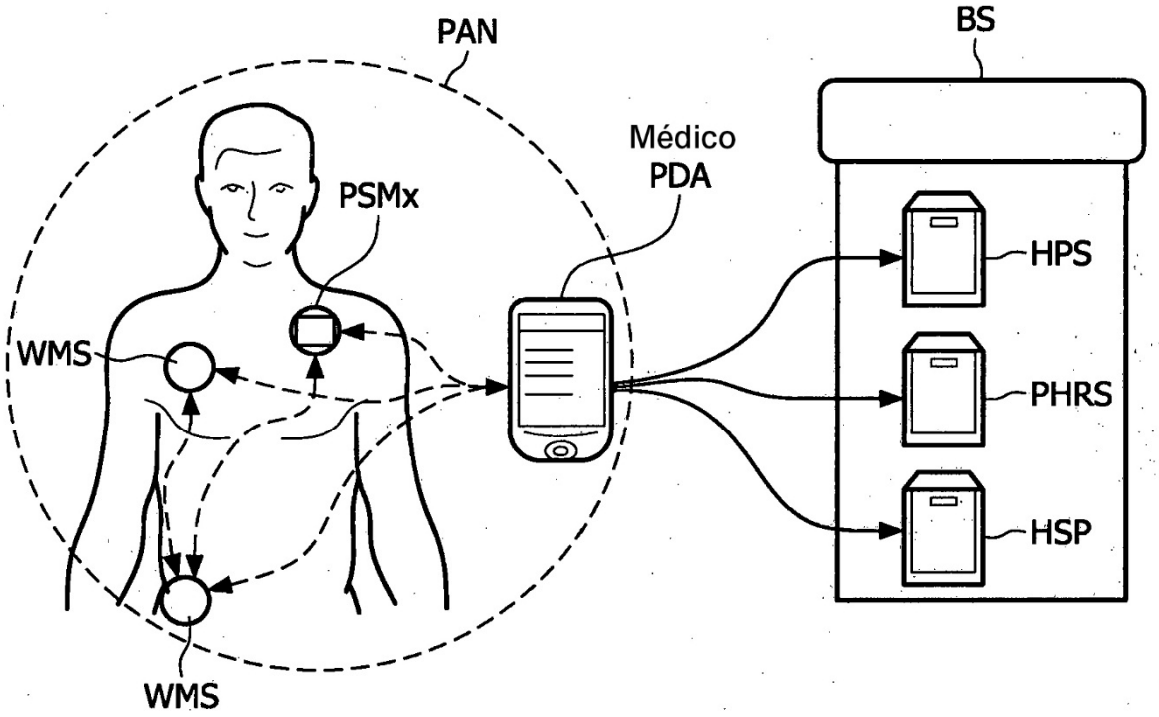

FIG. 7

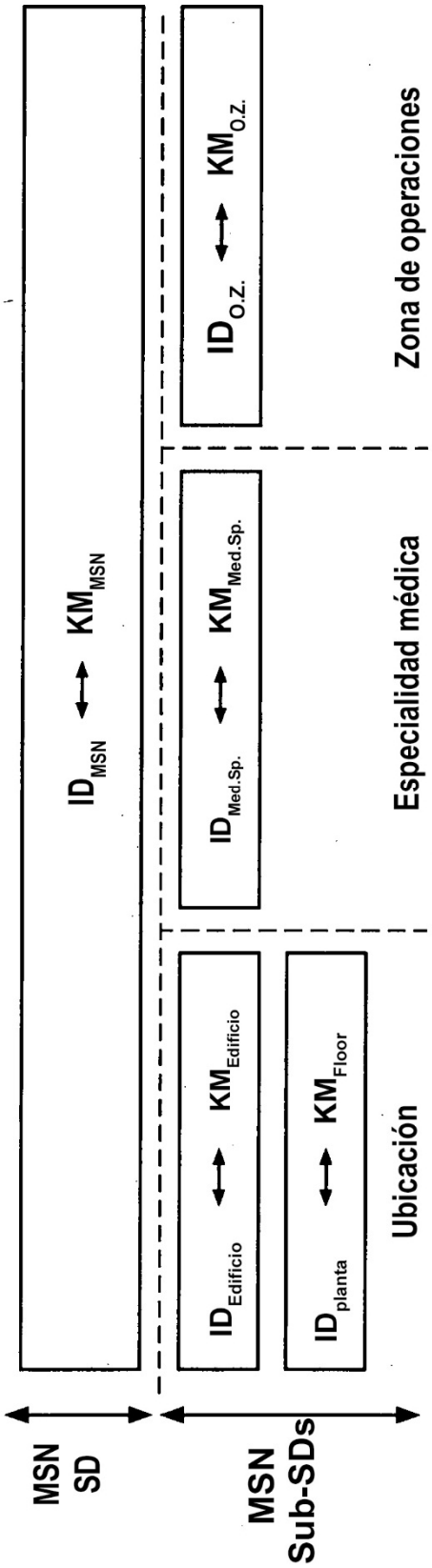
MSN
SD
MSN
Sub-SDs
ID_MSN
KM_MSN
ID_Edificio
KM_Edificio
ID_planta
KM_Floor
Ubicación
ID_Med.Sp.
KM_Med.Sp.
Especialidad médica
ID_O.Z.
KM_O.Z.
Zona de operaciones

FIG. 8

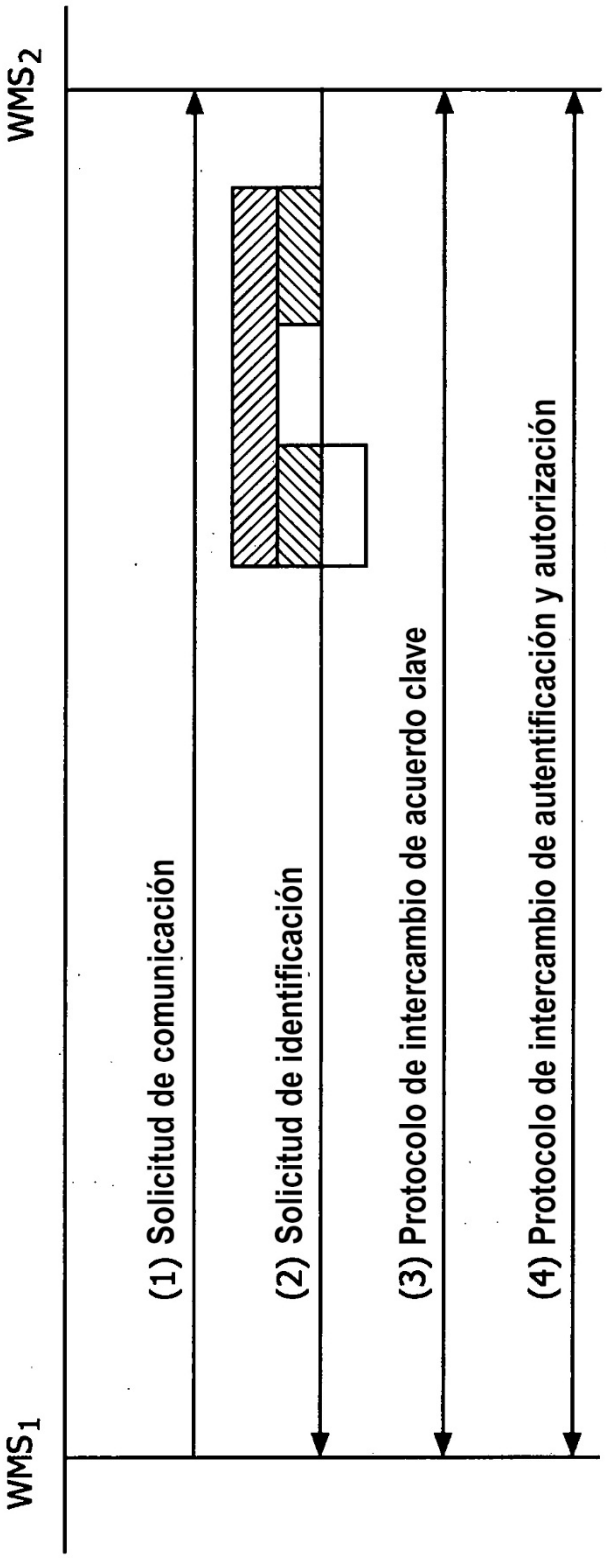
WMS2
WMS1
(1) Solicitud de comunicación
(2) Solicitud de identificación
(3) Protocolo de intercambio de acuerdo clave
(4) Protocolo de intercambio de autentificación y autorización

FIG. 9

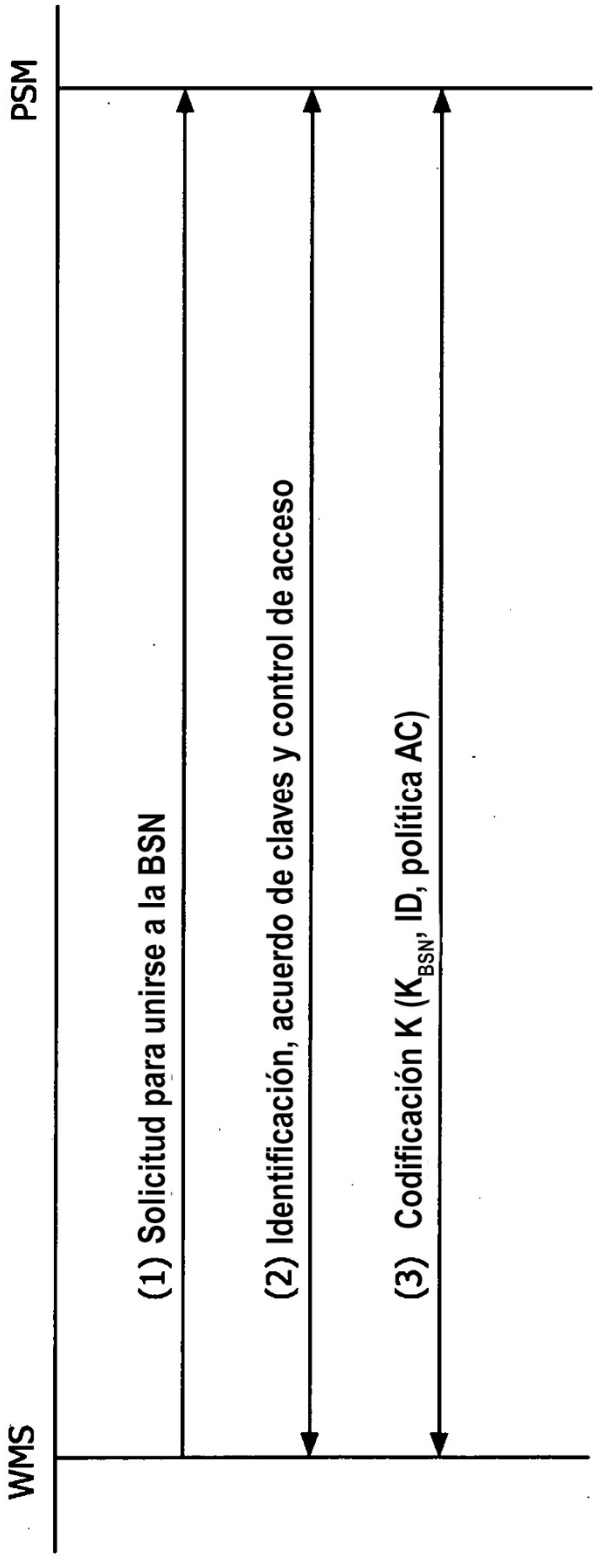
PSM
WMS
(1) Solicitud para unirse a la BSN
(2) Identificación, acuerdo de claves y control de acceso
(3) Codificación K (K_{BSN}, ID, política AC)

FIG. 10

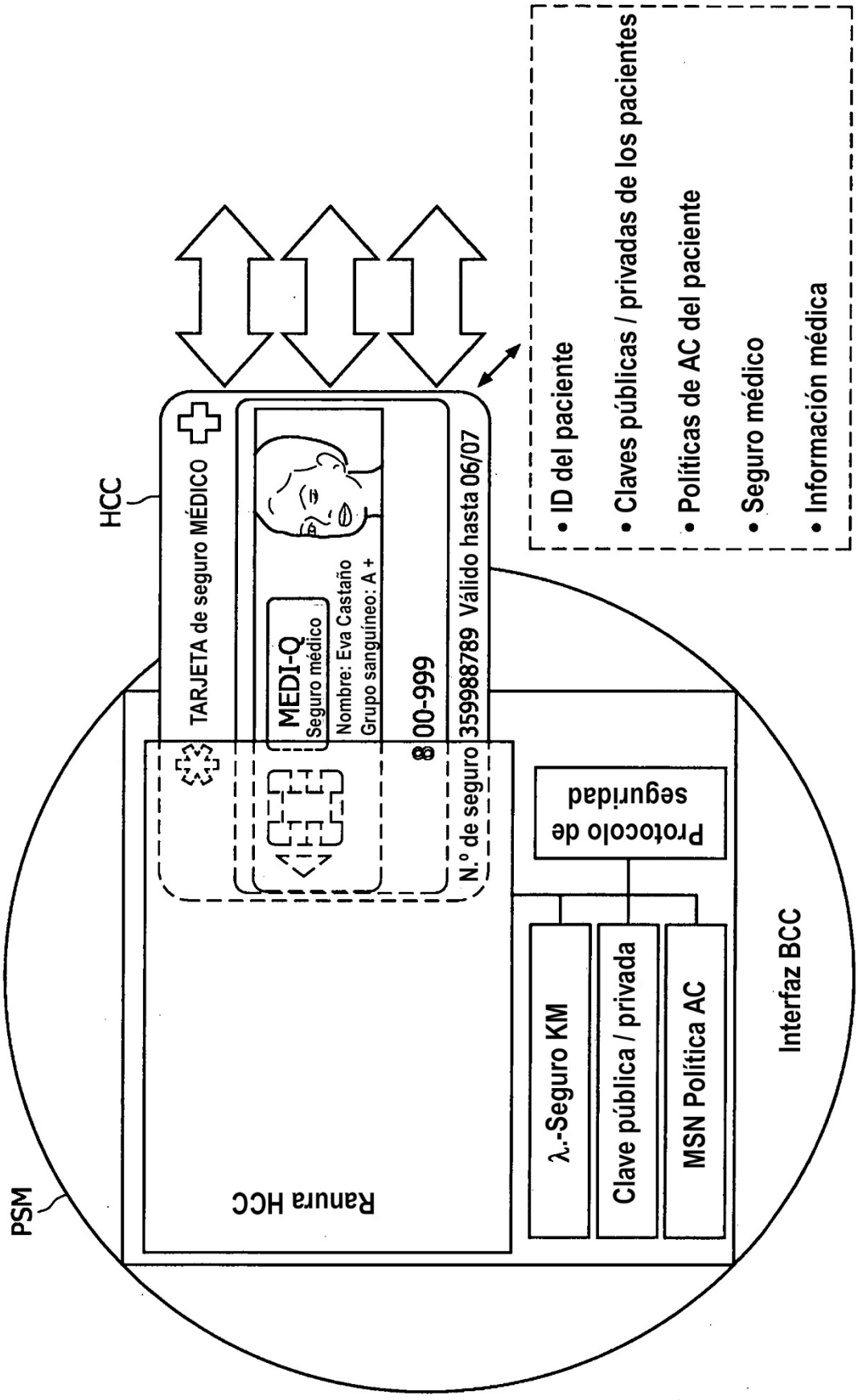
• ID del paciente
• Claves públicas / privadas de los pacientes
• Políticas de AC del paciente
• Seguro médico
• Información médica
HCC
TARJETA de seguro MÉDICO
MEDI-Q
Seguro médico
Nombre: Eva Castaño
Grupo sanguíneo: A +
800-999
359988789 Válido hasta 06/07
N.º de seguro
Ranura HCC
PSM
λ.-Seguro KM
Clave pública / privada
MSN Política AC
Protocolo de seguridad
Interfaz BCC

FIG. 11

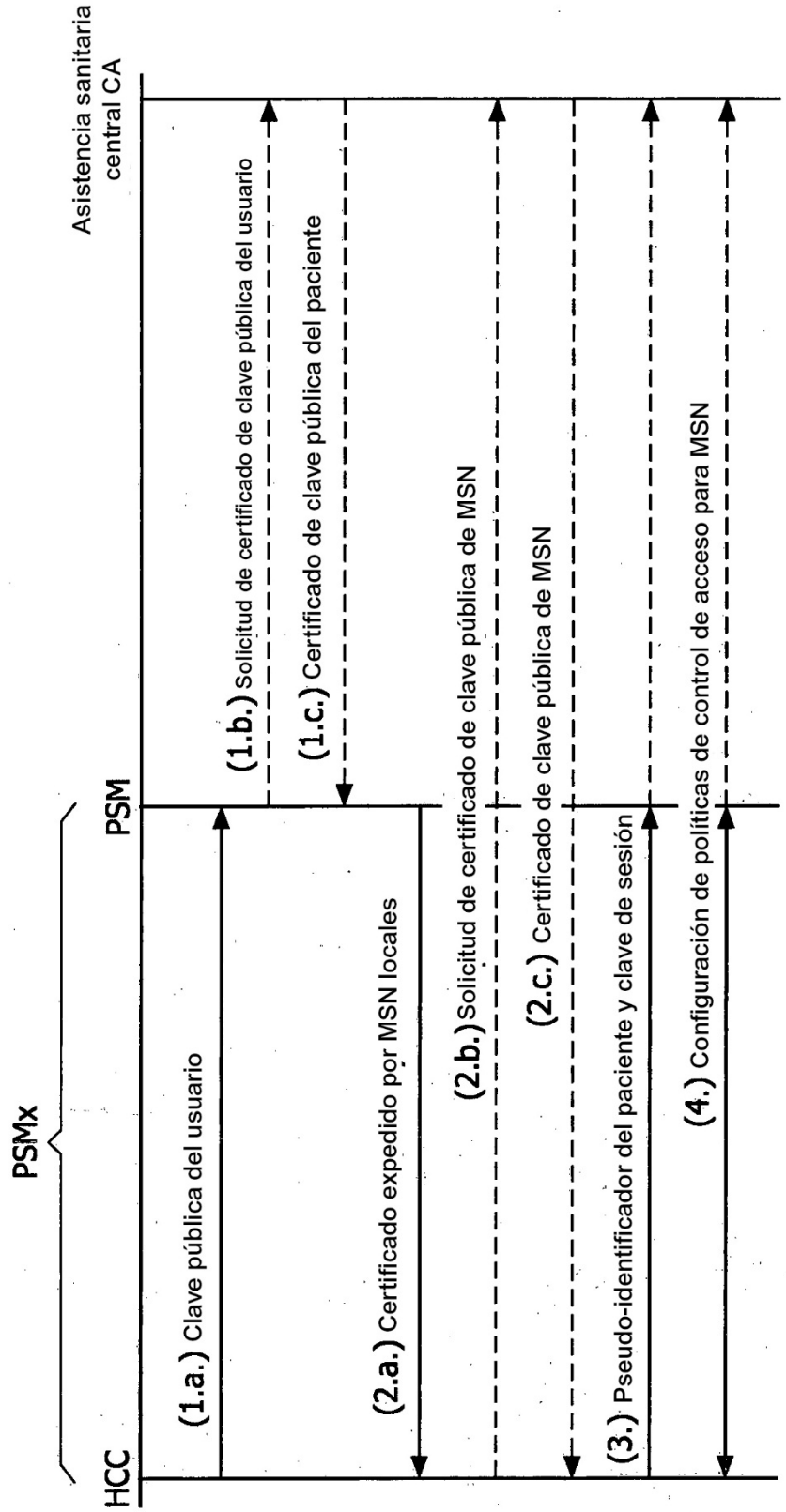
Asistencia sanitaria central CA
PSM
PSMx
HCC
(1.a.) Clave pública del usuario
(1.b.) Solicitud de certificado de clave pública del usuario
(1.c.) Certificado de clave pública del paciente
(2.a.) Certificado expedido por MSN locales
(2.b.) Solicitud de certificado de clave pública de MSN
(2.c.) Certificado de clave pública de MSN
(3.) Pseudo-identificador del paciente y clave de sesión
(4.) Configuración de políticas de control de acceso para MSN

FIG. 12

		TIEMPO (MS)	RAM (BYTES)	ROM (BYTES)	MATERIAL DE CLAVE (BYTES)
MICAz	RSA-1024 (CLAVE PÚBLICA)	430	542	1,073	128
	RSA-1024 (CLAVE PRIVADA)	10,990	930	6,292	128
	ECC SECP 160 R1	810	282	3,682	20
	ACUERDO DE CLAVE DISTRIBUIDA	$0.0625 \cdot \lambda$	20	416	$8 \cdot \lambda$
UPD789828	SHA 512 BITS	2	-	-	64
	ECDSA 255 SIGN	81	-	-	32
	ECDSA 255	380	-	-	32

FIG. 13

	Kbytes MEMORIA	N_{IJ}	α	α_r
SDMSN	800	1,000	100	0,1
$SD_{HOSPITAL}$	408	500	51	0,102
$SD_{DEPARTM.}$	224	100	28	0,28
SD_{OZ}	308	100	38,5	0,385
$SD_{MED.SPEZ}$	308	125	38,5	0,308
MλKE	2,048	-	385	0,385

FIG. 14